EUROPEAN UNION AGENCY
FOR CYBERSECURITY

STOCK TAKING OF SECURITY REQUIREMENTS SET BY DIFFERENT LEGAL FRAMEWORKS ON OES AND DSPS

The NISD and the GDPR

NOVEMBER 2019

ABOUT ENISA

The mission of the European Union Agency for Cybersecurity (ENISA) is to achieve a high common level of cybersecurity across the Union, by actively supporting Member States, Union institutions, bodies, offices and agencies in improving cybersecurity. We contribute to policy development and implementation, support capacity building and preparedness, facilitate operational cooperation at Union level, enhance the trustworthiness of ICT products, services and processes by rolling out cybersecurity certification schemes, enable knowledge sharing, research, innovation and awareness building, whilst developing cross-border communities. Our goal is to strengthen trust in the connected economy, boost resilience of the Union's infrastructure and services and keep our society cyber secure. More information about ENISA and its work can be found www.enisa.europa.eu.

AUTHORS
George Rousopoulos, Hellenic Data Protection Authority

EDITORS
Konstantinos Moulinos, ENISA

Athena Bourka, ENISA

Prokopios Drogkaris, ENISA

CONTACT
For contacting the authors, please use resilience@enisa.europa.eu.
For media enquiries, please use press@enisa.europa.eu.

ACKNOWLEDGEMENTS
Marnix Dekker, ENISA

Giuseppe D'Acquisto, Italian Data Protection Authority

Dina Kampouraki, EDPS

Massimo Rocca, ENEL

COPYRIGHT NOTICE

ISBN 978-92-9204-320-9, DOI 10.2824/73796

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Two legal acts that came into effect in 2018 contain obligations on information security. The General Data Protection Regulation (GDPR) has reinforced the pre-existing provisions of Directive 95/46/EC on security of personal data for data controllers and processors. The Network and Information Systems Directive (NISD) introduced obligations for operators of essential services (OES) and for digital service providers (DSP), in an effort to achieve a baseline, common level of information security within the European Union (EU) network and information systems.

Over the previous years, ENISA has published several guidance documents for security measures both in the context of the NISD, addressed to OESs and DSPs, and in the context of the GDPR, addressed to controllers and processors. Based on these publications, this report aims at providing a harmonized approach in using the available ENISA guidance, one that can also be used by every organisation that plans to implement security measures appropriate for the security of network and information systems as well as for personal data protection.

This report aims at providing a harmonized approach in using the available ENISA guidance on how to implement security measures for network and information systems as well as for personal data protection.

Although both NISD and GDPR follow a risk-based approach, the entities under the scope of these provisions should take into account the differences arising from: a) the scope of each legal instrument, b) the notion of risk within each legal instrument (e.g. risk for the organization and the risk for the individual), b) the purpose of deploying security measures, d) the (security) incidents under consideration and e) additional requirements, further to the risk assessment, imposed (e.g. Data Protection Impact Assessment (DPIA) which might be required under GDPR and pertains risk assessment),. The report establishes that, in practice, there is no conflict between these acts.

In order to support organisations in their process of identifying appropriate security measures, based on the provisions of both NISD and GDPR, this report uses as basis the pre-existing ENISA guidance and presents a mapping of already identified security objectives, between the NISD and the GDPR.

The report should be used as a starting point for the above-mentioned assessment and is targeted mainly to OESs and DSPs. Following the analysis in Sections 2, 3 and 4, this report concludes that organisations could benefit from a unified risk management framework, specialized sectorial guidance and specialised guidance on emerging privacy and security techniques. It also proposes that a method of cooperation between competent NISD and GDPR authorities as well as a co-ordinated approach on certifications concerning information security issues would be beneficial for the Digital Single Market.

Finally the report concludes a set of key recommendations which summarise as follows:

- NIS Competent Bodies and Data Protection Authorities should promote a common risk management framework risk because both NISD and GDPR follow a risk-based approach and managing risk can be achieved through one process.
- NIS Competent Bodies and Data Protection competent Authorities should follow a sector specific approach whenever this is required which takes into account the specific needs for information security as well as for data protection of the sector.
- Research Community and ENISA should continue to provide specialised guidance on emerging data protection and security techniques.

- NIS Competent Bodies as well as Data Protection Authorities, under the active leadership of European Commission should establish a method of collaboration in order to achieve consistency
- NIS Competent Bodies as well as Data Protection Authorities in collaboration with ENISA and European Commission should promote the collaboration of the NISD and GDPR in the area of certification.

1. INTRODUCTION

1.1 BACKGROUND

In May 2018, both the GDPR and the NISD came into force. The GDPR introduces reinforced information security requirements compared to Directive 95/46, for all organizations involved in personal data processing operations affecting EU residents. The NISD includes provisions on security requirements for OESs, designated per member state (MS) and DSPs, excluding micro and small enterprises.

Both EU legislations contain security requirements and require organizations to mitigate security breaches; however the focus of the NISD and the GDPR is different. The GDPR focuses on security breaches of personal data with an impact on individuals' rights and freedoms, while the NISD focuses on network and information security breaches with an impact on the services of OESs and DSPs.

The material scope of the NISD and the GDPR is also different. The GDPR applies to all organizations processing personal data while the NISD applies only to a subset of (large) companies. However, there are many organisations, which need to take into account both security requirements; for example, organisations which are not in scope of the NISD, but are delivering products and services to organisations in scope of this directive, say a small enterprise in the supply chain of an OES.

Since both legal acts share a common information security background, many of the security measures for OESs or DSPs under the NISD are also applicable for organizations under the GDPR. For instance, both legal instruments necessitate in practice the use of an information security management system and both follow a risk-based approach, even with a different orientation with regards to the impact, as under NISD the level of risk is calculated taking into account the impact on the organization while under GDPR the level of risk is calculated taking into account the impact on the individual.

1.2 SCOPE AND OBJECTIVE

The target audience of this publication is the information security personnel of OESs and DSPs.

The objectives of this report are to:

- demonstrate and analyse the different approaches of these two legislative documents as per the security requirements of network and information systems; and
- present a mapping of security objectives, between the NISD and the GDPR, based on existing ENISA publications.

It should be noted that this report focuses solely on network and information security requirements and should not be confused with requirements stemming from the data protection by design and by default obligation of the GDPR Article 25 or from a data protection impact assessment (DPIA - Article 35 GDPR) i.e. measures that are designed to implement, in an effective manner, data-protection principles, such as data minimisation. Indeed, while, a risk based approach, and deployment of relevant security measures, is part of the DPIA, additional aspects that go beyond information security must be taken into account while conducting a DPIA.

1.3 STRUCTURE

In section 2 an analysis of the legal framework for the NISD and the GDPR is presented, focused on the requirements for the security of network and information systems. Overlaps and gaps are identified and the main differences are pointed out. Section 3 provides a list of the main guidance documents that have been produced by ENISA and the NISD Cooperation Group, categorized by legal act.

Section 4 uses the aforementioned ENISA guidance to cover security requirements under both NISD and GDPR Finally, in section 5 we provide a list of conclusions and recommendations for future activities.

2. GAP ANALYSIS OF SECURITY RELATED PROVISIONS

2.1 THE EU LEGAL FRAMEWORK FOR THE SECURITY OF NETWORK AND INFORMATION SYSTEMS

Article 14 of NISD requires that member states (MSs) ensure that "…operators of essential services take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in their operations. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk posed." Furthermore, art. 15 para 2 (b) requires that OES need to have in place an "effective implementation of security policies".

In a similar way, Article 16 of NISD requires that MS ensure that "…digital service providers identify and take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in the context of offering services referred to in Annex III within the Union. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk posed, and shall take into account the following elements (a) the security of systems and facilities; (b) incident handling; (c) business continuity management; (d) monitoring, auditing and testing; (e) compliance with international standards."

The Commission issued implementing Regulation (EU) 2018/1511to further specify the elements that DSPs should take into account in order to manage the existing security risks of their networks and information systems, as well as the parameters for determining whether an incident has a significant impact or not.

For OES as well as for DSPs, the Directive aims to ensure the continuity of those services and to build a culture of network and information systems security across sectors vital for our society and economy and heavily dependent on ICT. NISD is applicable to industry sectors of Annex II while DSP services are stated in Annex III. The security measures are applicable only to the OES which will be designated as such by the MS. For this task, the Competent Authority (CA) should follow a consistent approach that is based on national criteria for the determination of what constitutes a significant disruptive effect. It is also evident that security requirements for digital service providers are lighter. In addition, micro and small enterprises are exempted from the NISD.

2.2 THE EU LEGAL FRAMEWORK FOR THE PROTECTION OF PERSONAL DATA

Security of personal data was already established as a legal obligation for data controllers under the Data Protection Directive 95/46/EC. GDPR reinforces the relevant provisions while extending this responsibility directly to data processors.

Security of personal data (but with a particular focus on integrity and confidentiality) is elevated in one of the principles relating to personal data processing (GDPR Article 5.1(f)). This puts security at the core of data protection together with the rest of data protection principles, i.e.

[1] http://data.europa.eu/eli/reg_impl/2018/151/oj

lawfulness, fairness and transparency, purpose limitation, accuracy and storage limitation. The addition of the accountability principle is also closely related to new obligations on security, as undertakings need not only apply security measures, but also mandatorily document them, i.e. through policies.

Section 2 of GDPR's chapter IV, spanning 3 specific articles, establishes obligations for data controllers and processors for the security of personal data processing including incident handling. GDPR Article 32 provides that "Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: (a) the pseudonymisation and encryption of personal data; (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing."

In the subsequent paragraph the article further defines the above introduced risk based approach, providing, in essence, risk factors: "in assessing the appropriate level of security account shall be taken in particular of the risks that are presented by data processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed". It also mentions the use of codes of conduct or certification mechanisms (as regulated in Article 41 GDPR) to demonstrate compliance with the requirements for the security of processing. Last, it states that the controller in primis and consequently the processor are responsible for their personnel as they are required to take steps to ensure that any natural person acting under their authority and who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law2.

It is worthwhile mentioning that the GDPR not only uses the classic CIA triad (confidentiality, integrity, availability) but also introduces "resilience" as the fourth constituent part of security. This recognises that reliability (e.g. fault tolerance, absence of single points of failure) of information systems processing personal data are important for the development of the digital economy and for the provision of services to EU residents. A perfect example for that argument is the importance of DSPs, as mentioned in NISD. For their proper functioning, these systems need also to withstand and recover from disruptions.

2.3 THE SECURITY PROVISIONS IN NISD AND GDPR

From the previous analysis it is evident that both legal texts follow a risk-based approach. This is not surprising. OESs and DSPs activities under the scope of the NISD and most personal data processing operations are carried out through information systems and networks. The principles of information security risk management are applied in both cases in order to identify, quantify and manage the security risks that an organisation faces. To be able to identify differences and similarities, we need to look at the purpose and scope of each legal act and check the following four factors:

1. Risks stemming from each legal act
2. The purpose of security measures
3. The scope of each legal act

[2] For an introduction to information security and risk management, examining the specificities for personal data processing see (ENISA, 2016B)

4. Security incidents under consideration

2.3.1 A risk-based approach

The NISD explicitly defines risk as "any reasonably identifiable circumstance or event having a potential adverse effect on the security of network and information systems" (Article 4.9 NISD). Incidents can impede the pursuit of economic activities, generate substantial financial losses, undermine user confidence and cause major damage to the smooth functioning of the economy within the Union. From the above, it is evident that the directive recognises that reliability and security of network and information systems and services are essential to economic and societal activities, and in particular to the functioning of the internal market. It is a risk framework based on operational aspects and losses, essentially economic in its nature.

NISD and GDPR require a proper assessment of security risks.

On the other hand, the GDPR relates risk to the rights and freedoms of individuals. This approach introduces the impact of a potential personal data breach to the data subjects as the major aspect of the data protection risk assessment and should also be seen in relation to the requirement for a formal data protection impact assessment (Article 35 GDPR). Risks are described in the regulation's recital 85 as "physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned". WP293 also states that these risks are linked not only to privacy but to the rights enshrined to the Charter of Fundamental Rights of the EU4. These risks include the "rights of the data subject" as provided in chapter II of the GDPR. These provisions directly affect information systems that process personal data, since procedures to access, rectify, erase or in some cases restrict operations in one's personal data, become mandatory requirements. It is a risk framework based on rights and freedoms, essentially legal in its nature.

Since, there is no "no one-size-fits-all approach" for the calculation of the security risk, the maximum possible level of harmonization and consistency[1] between security risk assessment methodologies under the two legal acts should be pursued.

The key question is whether there is a unified risk management framework to mitigate all risks or not. The following section explores possible answers to this question.

2.3.2 Security objectives

A risk management process comprises four key phases5, namely risk assessment, risk treatment, risk acceptance and risk communication. Since both the NISD and the GDPR follow a risk based approach, the aforementioned process can be followed, but one should bear in mind the particularities of each legislative act. Since risks are of different nature (the NISD focuses on societal and economic activities while the GDPR focuses on individual rights) measures appropriate to mitigate each risk might be different. For example, measures like pseudonymisation are mostly appropriate to data protection while measures and policies related to the (cyber) ecosystem and suppliers of OES are tailor made for that category of undertakings. It should be however noted that not all phases of risk management might be applicable when putting together the provisions of both legal instruments. For example, there may be cases under the GDPR that risk acceptance might not be a viable option[6].

In addition, the stakeholders involved in incident or data breach notifications are different. In case of a NISD security breach computer security incident response teams (CSIRTs) and CAs

[3] See (ARTICLE 29 DATA PROTECTION WORKING PARTY, 2018) and (ARTICLE 29 DATA PROTECTION WORKING PARTY, 2017A)
[4] The Charter of Fundamental Rights of the EU, available at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT
[5] See detailed analysis in ENISA's information packages for SMEs on risk assessment and risk management methods, https://www.enisa.europa.eu/publications/information-packages-for-small-and-medium-sized-enterprises-smes
[6] In this vein, it is worth mentioning article 36.1 of the GDPR that, in order to limit any hasty risk acceptance by data controllers, invokes the consultation of the supervisory authority whenever a data protection impact assessment indicates that the processing would result in a residual high risk in the absence of additional measures taken by the controller to mitigate the risk.

should be informed about incidents in order to be able to contribute to the overall national and EU cybersecurity. On the other hand, according to the GDPR, in case of personal data breaches, the controllers have to measure their impact and the level of risk to the fundamental rights of the affected individuals. Following that assessment, the supervisory authorities (SAs) and data subjects may be required to be informed in order to be able to mitigate the negative effects of the breach. CSIRTS and NISD CAs can communicate with OES, on their own initiatives, in their attempt to achieve a high level of security of network and information systems within the EU, or as a necessary precaution in case of a major incident.

It is up to Member States to define these cooperation procedures. This is not only stated in the NISD but also in GDPR. More specifically, recitals 5 and 7 of the GDPR emphasise on the importance of the free flow of personal data within the Union and the need to create an environment of trust that will allow the digital economy to develop across the internal market. The addition of resilience as a fourth element of security in GDPR is a clear indication of the interconnection between the two legal texts.

According to the NISD, competent authorities as well as data protection authorities should cooperate and exchange information on all relevant matters to tackle any personal data breaches resulting from incidents.

Although there are significant differences, regarding the security measures in scope.

NISD and GDPR share a common information security background.

The proper functioning of the underlying network and information systems and services is a prerequisite for the security of any data processing operation.

2.3.1 Scope

The NISD applies only to two broad categories of undertakings.

1. DSPs that provide important resources for their users in today's digital economy. Three categories of DSPs are considered (online marketplaces, online search engines and cloud computing services). Micro- and small enterprises are exempted.

2. OESs, that provide services "*essential to the maintenance of critical societal and/or economic activities*".

Online market places and online search engines are mostly addressed to individuals, so proper functioning of these undertakings is highly related to the protection of personal data. Cloud computing services might be addressed to individuals or offered to businesses, but it is also highly likely that they are used for personal data processing operations as well.

NISD covers all processing operations, including those with personal data, but only as long as they are critical for the provision of the undertaking's services.

On the contrary, GDPR is limited only to personal data processing operations, but it is applicable to every undertaking involved in such a processing operation, regardless of its size.

In the case of OESs, it is more complicated to come to a generic conclusion whether personal data processing is taking place due to a legal obligations, a legitimate interest, consent etc. The correlation of the critical operations of such an operator with personal data protection operations might vary drastically, depending on the nature of operations of each sector, the associated risks and the introduction of personal data processing techniques in their core operations. For example, the health sector is highly linked to personal data, while core operations of drinking water supply and distribution seem less dependent on personal data processing operations. However, the gradual introduction of new digital solutions, like IoT and smart metering, highly relying on individuals' habits, and the broad notion of personal data could lead to a change in the future, taking into account also the increased possibilities of indirect identification through data inference even when data de-identification techniques have been implemented (see (ENISA, 2015B)).

2.3.2 Security Incidents

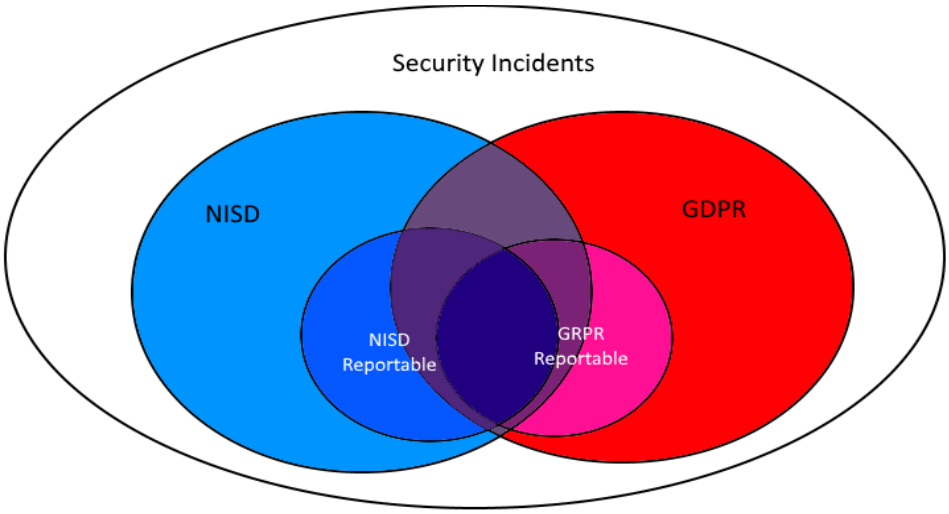
Under the NISD 'incident' means any event having an actual adverse effect on the security of network and information systems. Not all security incidents are within the scope of the NISD. The NISD Cooperation Group has identified that for OESs (NIS Cooperation Group, 2018B), incidents under scope are those affecting the availability, authenticity, integrity or confidentiality of networks and information systems (used in the provision of the essential service). In the case of DSPs the incident should have an impact on the availability, authenticity, integrity or confidentiality of the digital service. Incidents reported to a CA are those having a "*significant impact*" on the continuity of the essential service and those having a substantial impact on the provision of a digital service.

Under the GDPR a 'personal data breach' is defined as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed. In practice, incidents that fall under the GDPR are security incidents affecting personal data and that may impact individuals' rights and freedoms, so data breaches are a subset of security incidents. Reportable data breaches are those that are likely to result in a risk to the rights and freedoms of natural persons (see more details in (ARTICLE 29 DATA PROTECTION WORKING PARTY, 2018)).

In the context of this report, a security incident can be defined as an event that has an impact on the security of the network and information system or on the security of the digital service or on the processing of personal data. Organisations that face an incident will need to assess whether they are obliged to notify under each piece of legislation or not.

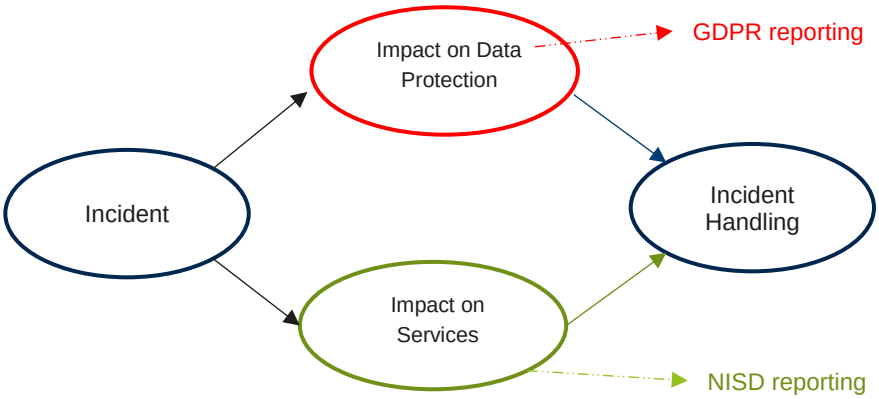
Organisations should also have in place procedures for the response, mitigation, recovery and remediation from such an incident.

Figure 1: Security incidents under NISD and GDPR.



These procedures can be harmonised to the maximum possible extent for the NISD as well as for the GDPR. For example, healthcare or cloud providers might increase data availability by duplicating data (thus reducing the likelihood of negative impacts on individuals arising from absence of a backup) or implementing multihoming on storage facilities (thus reducing the likelihood of negative impact on operations arising from an infrastructural failure). This way they could ensure continuity of the services offered and access to personal data, to meet the requirements arising from both legal acts.

Figure 2: Incident handling for NISD and GDPR



Despite their common elements, reporting procedures might also differentiate due to the impact of reporting periods on them. However, incident reporting and communicating procedures

(Articles 33 and 34 of the GDPR or articles 14(3) and 16(3) of the NISD) are outside the scope of this report and organisations should consult the already available guidance on the subject[7].

2.3.3 The use of an Information Security Management System

NISD provisions do not directly provide for the establishment of an information management system. However, since an obligation to have regard to the "state of the art" is explicitly stated, it is evident that the use of an information security management system is encouraged. That is also suggested by (NIS Cooperation Group, 2018A) and the Commission's Implementing Regulation (EU) 2018/151.

GDPR provisions on information security go beyond the mere adoption of specific security measures by supporting the establishment of a thorough information management system for the protection of confidentiality, integrity, availability and resilience of personal data. Article 32 of the GDPR explicitly provides for a process for testing, assessing and evaluating the effectiveness of the adopted information security measures, which indirectly calls for such an information security management system.

It is worthwhile noticing that security measures in the GDPR are also envisaged as means to demonstrate compliance with all principles of the Regulation[8], i.e. for the lawfulness of processing. For the purpose of this report, analysis is limited only to measures specifically linked to the security of information systems and to Article 32 of the GDPR without making a broad legal analysis of all the principles relating to processing of personal data.

Both legal acts require the use of an information security management system:

One explicitly for security of critical operations

The other for the protection of personal data processing. That is where both legal acts meet.

2.4 Summary

Following the analysis in the previous sections, Table 1 below provides a comparative summary of the NISD and GDPR security provisions.

Table 1: Summary of NISD and GDPR security provisions

Characteristic	NISD	GDPR
Risk focus	Essential or digital services	Data subjects' rights and freedoms
Security measures focus	Resilience	Data Protection
Scope	OES and DSP	All undertakings processing personal data
Security incidents	Significant impact on the service	Personal data breach
Need for an ISMS	Yes	Yes

2.5 ENISA Guidance Documents on NISD & GDPR Security Measures

Over the last years ENISA has published several guidance documents on security requirements in the context of the NISD as well as of the GDPR. In 2018, the NIS Cooperation Group issued a reference document on security measures for OES and Commission issued an Implementing Act on the elements to be taken into account by digital service providers for managing the risks posed to the security of network and information systems. Having noted that, the following is the list of documents which is the basis for the subsequent analysis.

1. Commission Implementing Regulation (EU) 2018/151 laying down rules for application of Directive (EU) 2016/1148 of the European Parliament and of the Council as regards further specification of the elements to be taken into account by digital service

[7] See (ARTICLE 29 DATA PROTECTION WORKING PARTY, 2018), (NIS Cooperation Group, 2018B) and (NIS Cooperation Group, 2018C)
[8] See Articles 24.1 and 35.7 of the GDPR

providers for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a substantial impact.

2. ENISA 'Technical Guidelines for the implementation of minimum security measures for Digital Service Providers', (ENISA 2016A)
3. The NIS Cooperation Group Publication 01/2018 - Reference document on security measures for Operators of Essential Services
4. ENISA, 'Guidelines for SMEs on the security of personal data processing', (ENISA 2016B)

A brief presentation of these documents takes place in the next sections.

2.6 Guidelines relevant to NISD security measures

Commission Implementing Regulation (EU) 2018/151 specifies five (5) security elements to be taken into account by DSPs to achieve a high common level of security of network and information systems. This Regulation states high level objectives that DSPs must mandatorily use when identifying the appropriate technical and organizational measures, using a risk based approach.

In (ENISA, 2016A) common baseline security objectives for DSPs are defined. This study lists 27 security objectives (SOs) for DSPs. In those 27 SOs, security measures are included and are set against well-known industry standards, national frameworks and certification schemes.

The NIS Cooperation Group issued a reference document on security measures for OES (NIS Cooperation Group, 2018A). In this report the group, taking into account the views of all MSs, including the specific implementation of security measure provisions in their national legislation, agreed on seven principles and suggested a list of security measures' domains. Within each domain the group abstractly described security requirements.

2.7 Guideline relevant to GDPR security measures

In (ENISA, 2016B) the Agency provides guidance tailored for SMEs, following a risk-based methodology. Since SMEs do not always have the necessary expertise and resources to perform a proper risk assessment, this study aims to facilitate them in understanding the context of personal data processing operations and subsequently assess the associated security risks. Organizational and technical security measures for the protection of personal data, which are appropriate to the risk presented, are proposed. These measures can be adopted by SMEs in order to achieve compliance with the GDPR's "no one-size-fits-all approach". SMEs have to identify the level of risk, depending on nature, scope, context of processing along to the types and volumes of data processed. Then, security measures are proposed, in order to mitigate the identified threats.

2.8 How enterprises can consult the available guidance?

As mentioned earlier, the starting point for OESs and DPSs should be the guidance produced by ENISA and the NISD CG. More specifically (ENISA, 2016A) interpreted in the light of the Commission Implementing Regulation (EU) 2018/151, should be the starting point for DSPs, while (NIS Cooperation Group, 2018A) should be the starting point in the case of OES. Taking the security objectives described in those reports as the baseline, the requirements of GDPR as presented in (ENISA, 2016B) can be analysed against them, in order to identify the areas where NISD security measures should be enhanced, for an operator/provider to be also compliant with data protection provisions. Although the above guidance has been produced having OESs and DSPs in mind, the proposed approach can also be used for every organisation that plans to implement security measures covering also the protection of personal data.

Do notice, that this approach can be used only for determining the proper security measures for the processing operations that involve personal data and does not cover all stages of the proper design and implementation of a data processing operation, including a data protection impact assessment.

3. SECURITY REQUIREMENTS

3.1 Mapping of security measures stemming from Commission's Implementing Regulation (EU) 2018/151

3.1.1 How to use the tables

Categories of security measures present in the guidance documents (ENISA, 2016A) and (ENISA, 2016B) cover, similar or even the same security objectives. For more guidance and possible levels of sophisticated implementation of the security measures, the DSP should consult the detailed guidance documents. One should also seek specialised guidance on topics of particular importance to data protection in the documents published by the EDPB, WP29 and the Commission both in the context of the GDPR e.g. guidance on data breaches, data portability and in the context of specific data processing operations e.g. cloud providers, transfers to third countries, processing data of employees or the use of CCTV systems.

3.1.2 Security requirements for DSPs tables

Commission Implementing Regulation (EU) 2018/151 dictates five (5) security mandatory elements for DSPs. The related guidance, namely (ENISA, 2016A), identified 27 Security Objectives (SOs), with the aim to cover all categories of security measures relevant to a DSP's resilience.

In the following table the SOs are grouped by the elements specified in the Implementing Regulation. To facilitate the reader, in the second column we provide the title of the SO, followed by the specific provision on the Implementing Regulation that it aims to cover (enclosed in parenthesis). The last part of the second column, enclosed in square brackets, lists the SOs number, following the numbering of (ENISA, 2016A). For the same purpose, the third column provides the short description of that particular SO, as presented in that paper.

The next step is to map this set of measures with those presented in (ENISA, 2016B) which are related to data protection. Each SO is analysed and enhancements are proposed to encounter the differences in the security objectives arising from the (ENISA, 2016B). A brief justification of the proposal is given followed by a reference (in parenthesis) to the specific security category or categories, as presented in (ENISA, 2016B), that correspond to this security measure.

To summarise the use of this table, the DSP should:

1. Start from (ENISA, 2016A) and then assess whether existing security measures can successfully mitigate the risks on the networks and information systems by using the second column of the table.
2. Understand the additional elements required for this specific measure in order to mitigate the risks on personal data by reading the last column of the table.
3. Get deeper guidance on how this enhancement might be implemented from (ENISA, 2016B).

3.1.1.1 Security of Systems and facilities

S/N	Security Objective	Description (ENISA, 2016A)	Data protection requirements (ENISA, 2016B)
1.	Information Security Policy (art 2.1.a – managing information security) [SO 01]	The DSP shall establish and maintain an information security policy. The document details information on main assets and processes, strategic security objectives.	Information System Security Policy should also explicitly address the protection of personal data. (4.1.1.1)
2.	Risk Management (art 2.1.a – risk analysis) [SO 02]	The DSP shall establish and maintain an appropriate governance and risk management framework, to identify and address risks for the security of the offered services. Risk management procedures can include (but are not limited to), maintaining a list of risks and assets, using Governance Risk management and Compliance (GRC) tools, Risk Assessment (RA) tools, etc.	The conducted risk analysis should cover risks to the rights and freedoms of natural persons and consider the specificities of risk management for personal data processing. In some cases, a Data Protection Impact Assessment could be mandatory. Consider using DPIA tools and data protection risk assessment methodologies[9]. (2.3.2, 3)
3.	Roles and Responsibilities (art 2.1.a – human resources) [SO 03]	The DSP shall assign appropriate security roles as well as security responsibilities to designated personnel (i.e. CSO, CISO, CTO etc.).	Personnel with access to personal data should have clearly defined and documented responsibilities. Relevant roles shall be based on a need to know basis and frequently been reviewed. Consider the appointment of a DPO[10], which could be obligatory under article 37 of the GDPR[11]. (4.1.1.2)
4.	Background checks (art 2.1.a - human resources) [SO 05]	The DSP shall perform appropriate background checks on personnel (employees, contractors and third party users) before hiring, if required, for their duties and responsibilities provided that this is allowed by the local regulatory frame-work. Background checks may include checking past jobs, checking professional references, etc.	Background checks and any other processing of employees data for security purposes should be in line with GDPR. Relevant guidance from DPAs should be consulted [12]
5.	Security *and Data Protection* knowledge and training (art 2.1.a - human resources) [SO 06]	The DSP shall verify and ensure that personnel have sufficient security. Personnel shall be provided with regular training, appropriate to their role. This is for example achieved through awareness raising, security education, personnel training etc.	Personnel involved in the processing of personal data shall be properly informed about their duties to confidentiality and their data protection obligations. Training, also on a periodic basis where appropriate, should be targeted to personnel's roles, especially for key personnel involved in high risk processing. (4.1.3.1, 4.1.3.2)

[9] For DPIA guidance see (ARTICLE 29 DATA PROTECTION WORKING PARTY, 2017A)
[10] Caution should be taken, since it likely that DSPs, depending on their processing operations can be obliged to appoint a DPO according to GDPR article 37.
[11] For DPO guidance see (ARTICLE 29 DATA PROTECTION WORKING PARTY, 2017B)
[12] Guidance on the processing of personal data at the workplace is available in (ARTICLE 29 DATA PROTECTION WORKING PARTY, 2001), (ARTICLE 29 DATA PROTECTION WORKING PARTY, 2002) and (ARTICLE 29 DATA PROTECTION WORKING PARTY, 2017C)

S/N	Security Objective	Description (ENISA, 2016A)	Data protection requirements (ENISA, 2016B)
6.	Personnel changes (art 2.1.a - human resources) [SO 07]	The DSP shall establish and maintain an appropriate process for managing changes in personnel or changes in their roles and responsibilities.	The same SO is applicable to systems supporting personal data processing. (4.1.1.2, 4.1.1.3)
7.	Operating procedures (art 2.1.a – security of operations) [SO 12]	The DSP shall establish and maintain procedures for the operation of key network and information systems by personnel (i.e. operating procedures, user manual, administration procedures for critical systems etc.)	The same SO is applicable to systems supporting personal data processing. (4.1.1.1). Any update on operating procedures, user manual, administration procedures for critical systems should be delivered to the relevant personnel quickly and in a push mode.
8.	Integrity of network components, information systems *and system entry points* (art 2.1.a – security architecture) [SO 11]	The DSP shall establish, protect and maintain the integrity of its own network, platforms and services by taking steps to prevent security incidents. The goal is the protection from viruses, code injections and other malware that can alter the functionality of the systems or integrity or accessibility of information. All information systems should be considered.	The same SO is applicable to systems supporting personal data processing; especially on system, entry points e.g. servers and workstations. Mobile/portable devices increase exposure to theft and accidental loss of personal data and should be treated with extra care with use policy and, where appropriate, platforms for the remote management of terminals. (4.2.3, 4.2.4, 4.2.6)
9.	Change management (art 2.1.a – system life cycle management) [SO 13]	The DSP shall establish and maintain change management procedures for key network and information systems. These may include for example, change and configuration procedures and processes, change procedures and tools, procedures for applying patches etc.	The same SO is applicable to systems supporting personal data processing. Change management procedures should also focus on mitigating the risks of unauthorised disclosure, modification or destruction of personal data. (4.1.1.5)
10.	Asset management (art 2.1.a - system life cycle management) [SO 14]	The DSP shall establish and maintain asset management procedures and configuration controls for key network and information systems.	The same SO is applicable to systems supporting personal data processing. IT resources should include the means of personal data processing. (4.1.1.4)

S/N	Security Objective	Description (ENISA, 2016A)	Data protection requirements (ENISA, 2016B)
11.	Security of data at Rest (art 2.1.a – secure data) [SO 23]	The DSP establishes and maintains procedures for the protection of data at rest	The same SO is applicable to systems supporting personal data processing, especially servers, databases, workstations and mobile/removable devices (e.g. through hardening and encryption or data pseudonymisation) (4.2.3)
12.	Application lifecycle security (art 2.1.a – system life cycle management) [SO 25]	The DSP establishes and maintains a policy, which ensures that applications are developed in a manner which respects security.	Application development should respect the principles of data protection by design and by default[13]. All personal data processing operations should be designed with data protection in. The use of privacy enhancing techniques is recommended (4.2.7)
13.	Physical and environmental security (art 2.1.b) [SO 08]	The DSP establishes and maintains policies and measures for physical and environmental security of data canters such as physical access controls, alarm systems, environmental controls and automated fire extinguishers etc.	The same S**O is applicable to systems supp**orting personal data processing. The use of physical security measures entailing processing of personal data (e.g. biometrics, CCTV systems) should be in line with the GDPR (4.2.9)14
14.	Security of supporting utilities (art 2.1.c) [SO 09]	The DSP establishes and maintains appropriate security measures to ensure the security of supporting utilities such as electricity, fuel, HVAC etc. For example, this may be through the protection of power grid connections, diesel generators, fuel supplies, etc.	The same SO is applicable to critical systems supporting personal data processing. The use of mutual authentication between network and devices is recommended

[13] See GDPR article 25, (ENISA, 2014B) and (ENISA, 2018D)
[14] For CCTV guidance see (ARTICLE 29 DATA PROTECTION WORKING PARTY, 2004).

S/N	Security Objective	Description (ENISA, 2016A)	Data protection requirements (ENISA, 2016B)
15.	Third party management (art 2.1.c) [SO 04]	The DSP establishes and maintains a policy with security requirements for contracts with suppliers and customers. SLAs, outsourcing agreements etc., are established to ensure that the dependencies on suppliers and residual risks do not negatively affect security of the offered services.	Third party relations should necessarily be governed by contract or other legal act. Contracts should include specific clauses referring to the rules of processing of the security of personal data and the management of personal data breaches.[15] Further attention is required when personal data are transferred to third parties (data processors) in third countries (outside the E.E.A.)[16]. (4.1.1.6)
16.	Access control to network and information systems (art 2.1.d) [SO 10]	The DSP establishes and maintains appropriate policies and measures for access to business resources. For example, zero trust model, ID management, authentication of users, access control systems, firewall and network security etc.	The same SO is applicable to systems supporting personal data processing. Access to these systems should be based on the 'need to know' principle. See also (ENISA, 2018B) pp.18-27 for an analysis of different types of access control systems. (4.1.1.3, 4.2.1)
17.	Interface security (art 2.1.d) [SO 24]	The DSP should establish and maintain an appropriate policy for keeping secure the interfaces of the services that use personal data.	The same SO is applicable to systems supporting personal data processing. (4.2.4)
+	*Data deletion / disposal*	*The DSP establishes a data deletion and equipment disposal policy.*	The establishment of a personal data archiving and deletion as well as equipment disposal policy is an obligation arising from GDPR's principle of storage limitation and the obligation to respond to a data subject request under article 17, where applicable. (4.2.8)

[15] GDPR article 28 para 3 provides for specific clauses in contracts
[16] For the international dimension of data protection see https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection_en

3.1.1.2 Incident Handling

S/N	Security Objective	Description (ENISA, 2016A)	Data protection requirements (ENISA, 2016B)
1.	Incident detection & Response (art 2.2.{a,c,d}) [SO 15]	The DSP establishes and maintains procedures for appropriately detecting and responding to security incidents. These should consider detection, response, mitigation, recovery and remediation from such an incident. Lessons learned should also be adopted by the service provider.	Appropriate procedures should also be in place for detecting and responding to personal data breaches in particular when data processors are involved. For detailed guidance, see the relevant text endorsed by the EDPB[17]. (4.1.2.1)
2.	Incident reporting (art 2.2.b) [SO 16]	The DSP establishes and maintains appropriate procedures for reporting and communicating about security incidents and.	Appropriate procedures, including an assessment of the impact of a personal data breach on the fundamental rights of the individuals, should also be in place for reporting breaches to the competent SAs and possibly, in case of more severe risks, to the affected individuals (4.1.2.1)

3.1.1.3 Business Continuity Management

S/N	Security Objective	Description (ENISA, 2016A)	Data protection requirements (ENISA, 2016B)
1.	Business continuity (art 2.3.a) [SO 17]	The DSP establishes and maintains contingency plans and a continuity strategy for ensuring continuity of the services offered.	The same SO is applicable to systems supporting personal data processing with the goal to restore availability and access to personal data in a timely manner. Plans should also cover services critical for responding to data subjects rights requests (4.1.2.2)
2.	Disaster recovery capabilities (art 2.3.b) [SO 18]	The DSP establishes and maintains an appropriate disaster recovery capability for restoring the in case of natural and/or major disasters.	As above, the same SO is applicable to systems supporting personal data processing with the goal to restore availability and access to personal data in a timely manner (4.1.2.2, 4.2.5)

[17] See the relevant guidelines in (ARTICLE 29 DATA PROTECTION WORKING PARTY, 2018)

3.1.1.4 Monitoring, Auditing and Testing

S/N	Security Objective	Description (ENISA, 2016A)	Data protection requirements (ENISA, 2016B)
1.	Monitoring and logging (art 2.4.a) [SO 19]	The DSP establishes and maintains procedures and systems for monitoring and logging of the offered services and user actions (logs of user actions, system transactions/performance monitors, automated monitoring tools etc.).	The same SO is applicable to systems supporting personal data processing. Note that processing of personal data for monitoring and logging should be in line with GDPR (4.2.2)
2.	System tests (art 2.4.b) [SO 20]	The DSP establishes and maintains appropriate procedures for testing key network and information systems underpinning the offered services.	The same SO is applicable to systems supporting personal data processing. When possible, testing procedures should respect the principle of data minimization, e.g. by using dummy data.
3.	Security assessments (art 2.4.c) [SO 21]	The DSP establishes and maintains appropriate procedures for performing security assessments of critical assets.	The same control is applicable to systems supporting personal data processing
4.	Customer Monitoring and log access (art 2.4.c) [SO 27]	The cloud provider grants customers access to relevant transaction and performance logs so customers can investigate issues or security incidents when needed.	The same SO is applicable to systems supporting personal data processing. Notice also that relation between a cloud provider acting as data processor on the basis of instructions given by its customers (data controllers), should be governed by a written contract, according to the GDPR art. 28.

3.1.1.5 Compliance with (Inter) national Standards

S/N	Security Objective	Description (ENISA, 2016A)	Data protection requirements (ENISA, 2016B)
1.	Compliance (art 2.5) [SO 22]	The DSP establishes and maintains a policy for checking and enforcing the compliance of internal policies against the national and EU legal requirements and industry best practices and standards. These policies are reviewed on a regular basis.	The same SO is applicable to systems supporting personal data processing. Compliance with GDPR obligations should be a core element to this end.
2.	Interoperability and portability (art 2.5) [SO 26]	Online market place and cloud providers use standards which allow customers to interface with other digital services and/or if needed to migrate to other providers offering similar services.	The GDPR provides also for the right to portability[18]. For detailed guidance see the relevant text endorsed by the EDPB[19].

[18] This is also linked to the "Right to data portability" established for individuals by GDPR article 20. Do notice that this right does not create a direct and absolute obligation to data controllers to transfer data to another controller, but only when it is technically feasible.
[19] See (ARTICLE 29 DATA PROTECTION WORKING PARTY, 2016)

3.2 Mapping of security measures stemming from Cooperation Group's guidance

3.2.1 How to use the tables

Typically, OESs belong to the class of large companies and are vital for the modern society and the economy. Their operation is heavily dependent on ICT. However, they do not always rely on personal data processing. Specialized security standards have been in place for many years for each of these sectors[20], while some of the sectors are also regulated from sectoral national authorities. In addition, the level of dependence of each sector on ICT and the level of correlation of each section with personal data processing varies drastically. However, since both NISD and GDPR share a common information security background, categories of security measures, as presented in the table above, cover similar or even the same security objectives. We can distinguish in the following:

- Domains that need to take into account data protection risks. These mostly include domains related to Information System Security Governance, Risk Management, Ecosystem Management and Incident Management.
- Domains where the envisaged security objectives tend to be identical. Examples of these domains are asset management, IT security and administration domains, identity and access management and procedures related to IT maintenance, physical and environmental security and continuity of operations.
- Domains that are significantly critical for core OES activities. These domains include all measures related to industrial control systems, where limited data processing operations are expected, the level of logging analysis, which is dependent on the expected high risk, communication with CSIRSTs and crisis management.
- Domains that although, not included in the guidelines of the NIS Cooperation Group, should also be considered, in case of processing of personal data (marked with '+' in the table). In the table above, two such security objectives are added. The first relates to how an OES should develop (and not only maintain, that was already tackled) applications related to personal data, while the second is related to GDPR's principle of storage limitation.

Our goal is to provide a table that can be used as a reference. OESs should assess whether their existing security measures can successfully mitigate their risks, including those on data protection, using the table to identify the security measures that should be enhanced. In doing so, they need to analyse their operations and identify personal data processing activities that are critical for the provision of their services. Clearly, there is no "one-size-fits-all" solution, even within the same sector or subsector. For detailed guidance, operators should rely on appropriate sector specific security standards[21] and consult the available guidance documents.

3.2.2 Security requirements for OES

A similar approach for the security measures for OESs is proposed which uses the (NIS Cooperation Group, 2018A) as a starting point for this exercise. In this reference document, thirty (30) domains of security measures, divided into 4 parts, are identified. These domains are listed in the second column of the table and cover the broad spectrum of security measures relevant to an OES. The reader should consult the original document for the full description of the security measures. Similarly to the previous section, this set of measures is mapped with those presented in (ENISA, 2016B) which are related to data protection. Each measure is analysed and additional measures are proposed for personal data security. In the third column, a short description of the proposed enhancements accompanied by a reference –in parenthesis- to the relevant security measure, arising from (ENISA, 2016B), is provided.

[20] See (ENISA, 2017B) for a thorough presentation
[21] See (ENISA, 2017B)

To summarise the use of these tables, the OES should:

1. Start from (NIS Cooperation Group, 2018A) and assess whether existing security measures can successfully mitigate the risks on the networks and information systems by using the second column of the table.
2. Understand the additional elements required for personal data security by reading the last column of the table.
3. Get deeper guidance on how this data protection security requirements might be implemented from (ENISA, 2016B).

3.2.2.1 Governance and ecosystem

PART 1 – GOVERNANCE AND ECOSYSTEM		
1.1 INFORMATION SYSTEM SECURITY GOVERNANCE & RISK MANAGEMENT		
S/N	**Domain**	**Data protection requirements (ENISA, 2016B)**
1	Information System Security Risk Analysis	The conducted risk analysis should focus on the risks to the rights and freedoms of natural persons. If a Data Protection Impact Assessment was carried out[22], mandatorily or voluntarily, the outcome of this assessment can produce mandatory security measures to address the data protection risks. (2.3.2, 3)
2	Information System Security Policy	Information System Security Policy should also explicitly address the basic principles for the protection of personal data. (4.1.1.1)
3	Information System Security Accreditation	Data protection risks should be part of the accreditation process and data protection residual risks should be managed and documented. Attention should be paid to the possible need for DPIAs or consultation with the GDPR supervisory authority.
4	Information System Security Indicators	Indicators related to data protection risks should also be considered.
5	Information System Security Audit	Information system security assessments and audit procedures should consider data protection risks.
6	Human Resource Security	Personnel with access to personal data should have clearly defined and documented responsibilities. Relevant roles shall be based on a need to know and reviewed on a regular basis. Knowledge and training should be ensured for Confidentiality and Data Protection, according to personnel's roles. Personnel involved in the processing of personal data is properly informed about its duty to confidentiality and its data protection obligations. Training should be appropriate to personnel's roles, especially for key personnel involved in high risk processing. The role of the DPO includes, awareness-raising and training of staff involved in processing operations. (4.1.1.2, 4.1.3.1, 4.1.3.2)

[22] See GDPR article 35

7	Asset Management	The same control is applicable. IT resources should include the means of personal data processing. Formal internal accreditation procedure of most critical resources could be implemented. (4.1.1.4)
1.2 ECOSYSTEM MANAGEMENT		
1	Ecosystem Mapping	Ecosystem mapping should take into consideration the processing of personal data (e.g. processors, transfers to third parties). Relations concerning recipients of personal data shall be documented[23]. (4.1.1.6)
2	Ecosystem Relations	Third party relations should, necessarily, be governed by contract or other legal act. Contracts should include specific clauses[24] referring to the security of personal data and the management of personal data breaches. Further attention is required when personal data are transferred to third parties (data processors) in third countries (outside the E.E.A.) when chapter V of the GDPR applies[25]. (4.1.1.6)

3.2.2.2 Protection

PART 2 – PROTECTION		
2.1 IT SECURITY ARCHITECTURE		
S/N	**Domain**	**Data protection requirements (ENISA, 2016B)**
1	Systems Configuration	The same control is applicable to systems supporting personal data processing, especially system entry points e.g. servers, workstations and mobile devices (4.2.3, 4.2.6)
2	System Segregation	The same control is applicable to systems supporting personal data processing, especially servers and database servers. (4.2.3.1)
3	Traffic Filtering	The same control is applicable to systems supporting personal data processing. Traffic filtering and monitoring should be in line with GDPR [26]. (4.2.4)
4	Cryptography	Procedures related to the security of personal data should include privacy enhancing technologies, e.g. the use of encryption or pseudonymisation. Depending on the case, different techniques might be applicable[27]. (4.2.3.1, 4.2.4)

[23] This is an obligation arising from GDPR article 30.
[24] GDPR article 28 para 3 provides for specific clauses in contracts
[25] For the international dimension of data protection see https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection_en
[26] An assessment of processing operations resulting from monitoring ICT usage at the workplace can be found in (ARTICLE 29 DATA PROTECTION WORKING PARTY, 2017C) pp.12-15
[27] See more information on PETs in: https://www.enisa.europa.eu/topics/data-protection/privacy-enhancing-technologies and on cryptographic protocols and tools in https://www.enisa.europa.eu/topics/data-protection/security-of-personal-data/cryptographic-protocols-and-tools

2.2 IT SECURITY ADMINISTRATION		
1	Administration Accounts	The same control is applicable to administrators of systems supporting personal data processing. (4.1.1.3, 4.2.1)
2	Administration Information Systems	The same control is applicable to administrators of systems supporting personal data processing. (4.1.1.3, 4.2.1)
2.3 IDENTITY AND ACCESS MANAGEMENT		
S/N	**Domain**	**Data protection requirements (ENISA, 2016B)**
1	Authentication and Identification	The same control is applicable to accounts of systems supporting personal data processing (4.2.1)
2	Access Rights	The same control is applicable to accounts of systems supporting personal data processing. See also (ENISA, 2018B) pp.18-27 for an analysis of different types of access control systems. (4.1.1.3)
2.4 IT SECURITY MAINTENANCE		
1	IT Security Maintenance Procedure	The same control is applicable to systems supporting personal data processing. (4.1.1.5, 4.2.7)
2	Industrial Control Systems	Not applicable
+	Application lifecycle security	The OES should establish and maintain a policy which ensures that applications requiring processing of personal data are developed in a manner which is compliant to data protection and respects security, including the obligations of data protection by design and by default[28]. (4.2.7)
+	Data deletion / disposal	Where processing of personal data is required, the establishment of a personal data deletion and equipment disposal policy is an obligation arising from GDPR's principle of storage limitation. (4.2.8)
2.5 PHYSICAL AND ENVIRONMENTAL SECURITY		
1	Physical and Environmental Security	The same control is applicable to systems supporting personal data processing. The use of physical security measures entailing processing of personal data (e.g. CCTV systems) should be in line with GDPR (4.2.9)[29]

[28] See GDPR article 25, (ENISA, 2014B) and (ENISA, 2018D)
[29] For CCTV guidance see (ARTICLE 29 DATA PROTECTION WORKING PARTY, 2004). The EDPB has included videosurveillance guidelines in its work program for 2019/2020, so new guidance is expected

3.2.2.3 Defence

PART 3 – DEFENCE		
3.1 DETECTION		
S/N	**Domain**	**Data protection requirements (ENISA, 2016B)**
1	Detection	The same controls are applicable to systems supporting personal data processing. Analysis of data flows, logging and logs correlation should be in line with GDPR[30] . (4.2.2)
2	Logging	
3	Logs Correlation and Analysis	
3.2 COMPUTER SECURITY INCIDENT MANAGEMENT		
1	Information System Security Incident Response	Appropriate procedures should be in place for responding to personal data breaches[31]. (4.1.2.1)
2	Incident Report	Appropriate procedures, including an assessment of the effect of a breach to personal data, should be in place for reporting personal data breaches to the competent SAs and possibly to the affected individuals (4.1.2.1)
3	Communication with Competent Authorities and CSIRTs	See requirements for the notification of personal data breaches under GDPR.

[30] See (ARTICLE 29 DATA PROTECTION WORKING PARTY, 2017C) pp.12-15

[31] For detailed guidance see (ARTICLE 29 DATA PROTECTION WORKING PARTY, 2018)

3.2.2.4 Resilience

PART 4 – RESILIENCE		
4.1 CONTINUITY OF OPERATIONS		
S/N	**Domain**	**Data protection requirements (ENISA, 2016B)**
1	Business Continuity Management	The same control is applicable to systems supporting personal data processing with the goal to restore availability and access to personal data in a timely manner. Plans should also cover services critical for responding to data subjects rights requests (4.1.2.2)
2	Disaster Recovery Management	The same control is applicable to systems supporting personal data processing with the goal to restore availability and access to personal data in a timely manner (4.1.2.2, 4.2.5)
4.2 CRISIS MANAGEMENT		
1	Crisis Management Organization	The same control is applicable to systems supporting personal data processing. (4.1.2.2)
2	Crisis Management Process	The same control is applicable to systems supporting personal data processing. (4.1.2.2)

4. CONCLUSIONS - RECOMMENDATIONS

NISD and GDPR have both reinforced the provisions on information security, but from a different perspective. NISD aims to achieve a high level of resilience and security of network and information systems for entities that are essential for the functioning of the European economy, for the protection of critical services (e.g. health) as well as for the well-being of the citizen. GDPR aims to strengthen the protection of personal data, reinforcing the provisions on information security. Both legislative acts share a common information security background. Operators of Essential Services and Digital Service Providers face the burden of compliance with two sets of provisions with potential overlaps and unnecessary administrative burden.

This report aims to analyse the differences and similarities, based on ENISA technical documents, identify the overlaps and provide guidance to OESs, DSPs as well as to organisations that offer services to them, on how to implement technical and organisational measures that are appropriate for both set of provisions. Compliance cannot be merely formal or based on the implementation of closed checklists, but linked to the "context" where an operation takes place and the actual risks. Undertakings should follow methodologies that fit to their business sector to implement or assess their security measures, based on the pre-existing guidance. The proposed list of security objectives is aimed to provide a good starting point for this assessment.

While performing the analysis of selected measures categories, a number of conclusions and relevant recommendations were drawn and are discussed below.

A common risk management framework

Since both the NISD and the GDPR follow a risk based approach, managing risks can be achieved through one process by, taking into account security and data protection risks and their essential differences, especially on the way the risks are mitigated. Undertakings can benefit from a common risk management framework that uses common controls thus making it efficient and cost-effective, while at the same time making it easy to support risk management decisions. Notice that although there are security and privacy risk management frameworks[32], such an approach must be suitable for the EU legal framework and the notion of data protection as envisaged with the GDPR. Such a harmonised approach could also be beneficial to other legal frameworks that follow a risk based approach and can facilitate the establishment of the Digital Single Market.

Specialized guidance on each sector

From the analysis presented, it is obvious that the level of risk depends on the exact information (including personal data) processing activities and network dependencies of each entity. However, a contextual analysis of risks cannot be performed uniformly for every industry sector (or even subsector) that fall within the scope of the NISD. To further advance the level of security of network and information systems and data protection one needs to explore these activities and provide specialised guidance. A thorough analysis is required for each subsector,

[32] E.g. NIST SP 800-37 Rev. 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy - https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final

through cooperation of experts familiar with the particular subsector, security of network and information systems and data protection.

Specialised guidance on emerging data protection and security techniques

Competent EU bodies and research bodies should continue to provide specialised guidance on “state-of-the-art” data protection and security techniques. That will facilitate the adoption and deployment of these techniques throughout EU.

Synergies between NISD and GDPR authorities

NISD competent authorities (and CSIRTs) and Data Protection Authorities should also establish a method of cooperation, especially when dealing with security incidents. NISD provides for such a cooperation, but it is left up to national legislation. In order to achieve a consistent level of cooperation between these authorities, member states and authorities could benefit from a list of recommendations on how to establish synergies and put into practise collaborative and cooperative mechanisms.

Certifications

The new regulation on ENISA ("Cybersecurity Act") provides for a role of the agency on cybersecurity certification schemes. On the other hand, the GDPR provides for the establishment of certification mechanisms for its own purposes. A channel of co-operation between these two schemes could be explored in the future for the benefit of all involved parties in the area of information security.

5. REFERENCES

ARTICLE 29 DATA PROTECTION WORKING PARTY. (2001). *Opinion 8/2001on the processing of personal data in the employment context.* Retrieved from https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2001/wp48_en.pdf

ARTICLE 29 DATA PROTECTION WORKING PARTY. (2002). *Working documenton the surveillance of electronic communications in the workplace.* Retrieved from https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2002/wp55_en.pdf

ARTICLE 29 DATA PROTECTION WORKING PARTY. (2004). *Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance.* Retrieved from https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2004/wp89_en.pdf

ARTICLE 29 DATA PROTECTION WORKING PARTY. (2011). *Opinion 12/2011 on smart metering.* Retrieved from https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp183_en.pdf

ARTICLE 29 DATA PROTECTION WORKING PARTY. (2013A). *Opinion 04/2013on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems ('DPIA Template') prepared by Expert Group 2 of the Commission's Smart Grid Task Force.* Retrieved from https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp205_en.pdf

ARTICLE 29 DATA PROTECTION WORKING PARTY. (2013B). *Opinion 07/2013on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems ('DPIA Template') prepared by Expert Group 2 of the Commission's Smart Grid Task Force.* Retrieved from https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp209_en.pdf

ARTICLE 29 DATA PROTECTION WORKING PARTY. (2016). *Guidelines on the right to "data portability" (wp242rev.01).* Retrieved from https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233

ARTICLE 29 DATA PROTECTION WORKING PARTY. (2017A). *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 - Adopted on 4 April 2017, Revised and Adopted on 4 October 2017.* Retrieved from https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

ARTICLE 29 DATA PROTECTION WORKING PARTY. (2017B). *Guidelines on Data Protection Officers ('DPOs') (wp243rev.01).* Retrieved from https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048

ARTICLE 29 DATA PROTECTION WORKING PARTY. (2017C). *Opinion 2/2017 on data processing at work - wp249.* Retrieved from https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169

ARTICLE 29 DATA PROTECTION WORKING PARTY. (2018). *Guidelines on Personal data breach notification under Regulation 2016/679, Adopted on 3 October 2017, Revised and Adopted on 6 February 2018.* Retrieved from https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052

CNIL. (2018). *THE CNIL'S GUIDE ON SECURITY OF PERSONAL DATA.* Retrieved from https://www.cnil.fr/en/new-guide-regarding-security-personal-data

ENISA. (2012). *Appropriate security measures for Smart Grids, Guidelines to assess the sophistication of security measures implementation.* Retrieved from https://www.enisa.europa.eu/publications/appropriate-security-measures-for-smart-grids

ENISA. (2014A). *Technical Guideline on Security measures for Article 4 and Article 13a - Version 1.0, December 2014.* Retrieved from https://www.enisa.europa.eu/publications/guideline-on-security-measures-for-article-4-and-article-13a

ENISA. (2014B). *Privacy and Data Protection by Design – from policy to engineering.* Retrieved from https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design

ENISA. (2015A). *Information security and privacy standards for SMEs - Recommendations to improve the adoption of information security and privacy standards in small and medium enterprises.* Retrieved from https://www.enisa.europa.eu/publications/standardisation-for-smes

ENISA. (2015B). *Privacy by design in big data - An overview of privacy enhancing technologies in the era of big data analytics.* Retrieved from https://www.enisa.europa.eu/publications/big-data-protection

ENISA. (2016A). *Technical Guidelines for the implementation of minimum security measures for Digital Service Providers.* Retrieved from https://www.enisa.europa.eu/publications/minimum-security-measures-for-digital-service-providers/

ENISA. (2016B). *Guidelines for SMEs on the security of personal data processing.* Retrieved from https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing

ENISA. (2016C). *Privacy and Security in Personal Data Clouds.* Retrieved from https://www.enisa.europa.eu/publications/privacy-and-security-in-personal-data-clouds

ENISA. (2016D). *Cyber Security and Resilience of smart cars, Good practices and recommendations.* Retrieved from https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars

ENISA. (2017A). *Incident notification for DSPs in the context of the NIS Directive - A comprehensive guideline on how to implement incident notification for Digital Service Providers, in the context of the NIS Directive.* Retrieved from

https://www.enisa.europa.eu/publications/incident-notification-for-dsps-in-the-context-of-the-nis-directive/

ENISA. (2017B). *Mapping of OES Security Requirements to Specific Sectors.* Retrieved from https://www.enisa.europa.eu/publications/mapping-of-oes-security-requirements-to-specific-sectors/

ENISA. (2017C). *Handbook on Security of Personal Data Processing.* Retrieved from https://www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing

ENISA. (2018A). *Guidelines on assessing DSP and OES compliance to the NISD security requirements - Information Security Audit and Self – Assessment/ Management Frameworks.* Retrieved from https://www.enisa.europa.eu/publications/guidelines-on-assessing-dsp-security-and-oes-compliance-with-the-nisd-security-requirements

ENISA. (2018B). *Reinforcing trust and security in the area of electronic communications and online services - Sketching the notion of "state-of-the-art" for SMEs in security of personal data processing.* Retrieved from Reinforcing trust and security in the area of electronic communications and online services - Sketching the notion of "state-of-the-art" for SMEs in security of personal data processing

ENISA. (2018C). *Guidance and gaps analysis for European standardisation, Privacy standards in the information security context.* Retrieved from https://www.enisa.europa.eu/publications/guidance-and-gaps-analysis-for-european-standardisation

ENISA. (2018D). *Recommendations on shaping technology according to GDPR provisions - Exploring the notion of data protection by default.*

NIS Cooperation Group. (2018A). *Publication 01/2018 - Reference document on security measures for Operators of Essential Services.* Retrieved from http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=53643

NIS Cooperation Group. (2018B). *Publication 02/2018 - Reference document on Incident Notification for Operators of Essential Services - Circumstances of notification.* Retrieved from http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=53644

NIS Cooperation Group. (2018C). *Publication 06/2018 - Guidelines on notification of Digital Service Providers incidents - Formats and procedures.* Retrieved from http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=53675

NIST. (2018). *SP 800-37 Rev. 2 - Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy.* Retrieved from https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

Commission Implementing Regulation (EU) 2018/151 of 30 January 2018 laying down rules for application of Directive (EU) 2016/1148 of the European Parliament and of the Council as regards further specification of the elements to be taken into account by digital service providers for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a substantial impact

Annex: Terminology and Abbreviations

For brevity reasons the following terms and abbreviations are used throughout the report:

- OES: Operators of Essential Services.
- DSP: Digital Service Providers.
- NCA: National Competent Authority.
- IS: Information Systems.
- CIS: Critical Information Systems.
- EU MS: European Union Member States.
- ISO: International Organization for Standardization.
- NIST: National Institute of Standards and Technology.
- ISA: International Society of Automation.
- ICT: Information and Communication Technologies.
- NISD: The Directive on security of network and information systems
- GDPR: General Data Protection Regulation
- WP29: Article 29 Working Party
- EDPB: EU Data Protection Board
- SO: Security Objective
- SME: Small and Medium Enterprise
- SA: Supervisory Authority

MAKE SURE THAT THE OUTSIDE BACK COVER WILL BE A LEFT HAND PAGE. INSERT A BLANK RIGHT HAND PAGE IF NECESSARY.

TP-03-19-944-EN-N

ABOUT ENISA

The mission of the European Union Agency for Cybersecurity (ENISA) is to achieve a high common level of cybersecurity across the Union, by actively supporting Member States, Union institutions, bodies, offices and agencies in improving cybersecurity. We contribute to policy development and implementation, support capacity building and preparedness, facilitate operational cooperation at Union level, enhance the trustworthiness of ICT products, services and processes by rolling out cybersecurity certification schemes, enable knowledge sharing, research, innovation and awareness building, whilst developing cross-border communities. Our goal is to strengthen trust in the connected economy, boost resilience of the Union's infrastructure and services and keep our society cyber secure. More information about ENISA and its work can be found www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
1 Vasilissis Sofias Str
151 24 Marousi, Attiki, Greece

Heraklion office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

ISBN 978-92-9204-320-9
DOI 10.2824/73796