UiO : Faculty of Law
University of Oslo

Regulation of Encryption Under the GPDR and the NIS Directive

The Development of a ‘Cipherlaw’ for Businesses and Other Regulated Organisations

Candidate no.: 8014

Number of words: 16,789

Table of contents

Data is a precious thing and will last longer
than the systems themselves.
— Sir Tim Berners-Lee

1 Introduction[1]

Encryption has gone from being an advanced data security measure few people dealt with outside of the intelligence and cybersecurity communities, to become an everyday tool which is in use on most electronic appliances dependent on data storage and transfer today. Even so, its widespread usage goes largely unnoticed by the users, and is only superficially understood. More often than not this also applies to the businesses which rely on encryption to conduct their business in a secure manner.

This is changing, in large part due to security breaches affecting both private and government entities all around the world, leaving both personal data and business-critical information in the open, and the entities responsible having questions hurled at them and few answers beyond 'mea culpa'. Furthermore, there is a torrent of regulation raining down on all those entities, and subsequent challenges in implementing and complying with these. That is the subject of this thesis, where my research question will be as follows:

> *What level of encryption is required of organisations when they process data, both in transit and at rest, under the GDPR[2] and the NIS Directive[3]?*

The subject of the regulation I will examine are 'organisations', which is the deliberate wording used throughout in the relevant regulation[4]. This will effectively encompass all legal entities required to comply with the relevant regulation when it handles any type of data in a digital format.[5] I have also specified 'data in transit' and 'data at rest' as the most relevant data processing to regulate, and will expand on this in chapter 4.

---

[1] The quote by Tim Berners-Lee on the preceding page is sourced from *Harris and Maymi (2018)*, ch. 2. Berners-Lee is widely regarded as the inventor of the World Wide Web, or the internet as we best know it.

'Cipherlaw' (in the title) is a portmanteau of cyberlaw (a term often used for general IT law) and 'cipher', the core element of a cryptographic method (see chapter 3.1). It appears to have limited or no use in academic literature.

[2] *Regulation (EU) 2016/679* of the European Parliament and of the Council of 27 April 2016.

[3] *Directive (EU) 2016/1148* of the European Parliament and of the Council of 6 July 2016

[4] For the sake of simplicity, I will use the term *the relevant regulation* to refer to the articles in the GDPR (articles 5 (1) (f) and 32) and the NIS Directive (articles 14 and 16) of interest in this thesis. I will expand on the wording in the articles shortly.

Furthermore, I will refer to *regulation* in its broad sense, to be understood as the dictionary definition, not just as the type of EU law which e.g. the GDPR is categorised as, see e.g. *Oxford Dictionary of English (2015)*: 'a rule or directive made and maintained by an authority.'

[5] I have decided to use the neutral term 'organisation' for those legal entities which are regulated within computer security on a more general level. This is due to both the GDPR and the NIS Directive having a more general application, not limited to companies, businesses, or similar terms. They both in general refer to 'organisational measures', hence my decision to use this term throughout the thesis. In general, a small, or even one-

Organisations need to have a clear and understandable knowledge of what cybersecurity measures they are legally required to comply with, and cybersecurity regulation has made some important attempts at establishing such standards. But as we will see, these are deliberately flexible 'standards', revealing an open question as to what exactly may be considered sufficient encryption under the regulation put in place.

In cybersecurity regulation, the aim is to ensure the *confidentiality*, *integrity* and *availability* of the data being processed.[6] Encryption is primarily concerned with the *confidentiality* aim, in ensuring that the data can only be decrypted (and in turn, accessed in a sensible manner) by those persons authorised to do so. It must also ensure that the integrity of the data is maintained (that the decrypted data is the exact same data that was encrypted) and that those needing to and who are authorised to access the data may do so without unreasonable limitations. These latter two aims are important to consider when complete systems are to be designed and implemented to enable encryption. They fall, however, outside the scope of this thesis.

There are good reasons to encrypt data, as a data breach can be devastating to the organisations having data accessed without authorisation, let alone the data being stolen or deleted from their systems. Encryption radically reduces the consequences of a data breach, as correctly encrypted data requires the key to access it (which in a well-designed system will be stored elsewhere from the data itself).[7] Well-designed and implemented encryption is therefore a vital part of the systems of any organisation with a desire to protect the data which it stores, receives and sends against unauthorised access. However, the importance of such data goes beyond the interests of the organisation in question. This is why regulatory authorities are involving itself, and the reason why bad or lacking encryption may be a security flaw not only bad for business, but also bad for anyone wanting to be compliance with laws and regulation.

It is the aim of this thesis to find the level of security measures for encryption which may be understood to be required to comply with the regulation in the GDPR and the NIS Directive. While the GDPR deals with the security of personal data, the NIS Directive goes further, and (at least in theory) covers all types of data which an organisation may deal with. At the same time, the purposes of the NIS Directive are different than the GDPR, which I will expand on below. Even though the different types of data could imply different sets of protection (and in any case is based on a specific consideration of appropriateness), it is worth noting that the

person entity, are subject to the same regulation – even if the requirements to organisational measures must be understood as an analogy.

[6] See e.g., the *NIS Directive*, article 4 (2).

[7] See e.g., *Norsk kryptopolitikk (2019)*, p. 20.

wording towards what level of security is required is almost verbatim. This is the reason why I have decided to include both regulations – because it appears that the assessment on deciding on a level of encryption is substantially similar. I will revert to this point, but I wanted to emphasise how the similarities in wording is the main reason why I have chosen to deal with both. With this seemingly intended connection, comes also a more expansive framework of relevant sources, which I hope will give a more nuanced and insightful interpretation in the latter parts of the thesis.

This thesis is written from a Norwegian perspective, with the regulation under Norwegian law in mind. Sources are therefore based on a focal point of Norwegian legislation. However, as the core regulation I discuss in the thesis is EU law, one might reasonably consider the level of encryption the thesis seeks to recommend relevant for other national laws having implemented these regulations. It seems unlikely that this area should be any less in need of harmonisation than other policy areas in the EU. On the contrary – lacking encryption in some areas of the union, would be equally undesirable to all EU countries.

The next section of this assignment will deal with the methodology of this thesis, as well as the sources I have identified as relevant. I will then give a brief, but important overview of the technical aspects of cryptography and the main concepts the reader must both understand and have in mind for the remaining chapters. Based on the sources introduced in the methodology chapter, I will address the research question in the next part, where I will present the level of encryption the sources may suggest to be required under the regulations introduced. This will to some extent mirror the foregoing chapter, as there are many recommendations to be found throughout the technical literature – but our endeavour will be to find sound and authoritative recommendations throughout the relevant legal sources to establish the level of encryption which may be considered in compliance with the regulation at hand. Finally, I will discuss these findings and what their contents may imply for those organisations needing to find a suitable level of encryption.

2 Methodology and legal sources

2.1 The wording in the GDPR and the NIS Directive

The GDPR regulates the processing of personal data of all data subjects in the EU, both citizens and others. It is one of the strictest data privacy regulations that exists, at least considering the amount of people who are present in the EU at any one time. The GDPR contains regulation relating to the security of personal data processing in general, and encryption in particular. At

a higher level, it is apparent in one of the seven principles of personal data processing – the principle of integrity and confidentiality, as laid out in article 5 (1):

> 'Personal data shall be
> […]
> (f) processed in a manner that ensures **appropriate security of the personal data**, including **protection against unauthorised or unlawful processing** and against accidental loss, destruction or damage, using **appropriate technical or organisational measures** ("integrity and confidentiality").' (emphasis added)

This is further expanded on in article 32 on the 'Security of processing':

> '1. 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.
>
> 2. In assessing the appropriate level of security **account shall be taken** in particular of **the risks that are presented by processing**, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.
>
> 3. Adherence to an approved **code of conduct** as referred to in Article 40 or **an approved certification mechanism** as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.
>
> 4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor 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 law.' (emphasis added)

There are other articles of relevance in the GDPR which should also be mentioned, and a number of comments to be made on the contents of the two articles quoted, but I would first like to introduce some relevant sections from the NIS Directive.

The Network and Information Systems Security Directive (NIS) requires member states to establish minimum security requirements for information systems (ex ante-regulation), as well as required incident handling for security breaches (ex post-regulation). The NIS Directive differs between operators of essential services (OES) and digital service providers (DSP) in more stringent requirements to the former in both security measures and incident handling, ensuring that those entities having a more pivotal role to societal functions also have the corresponding level of security in place.[8] OES's are to be defined in and by each member state within the scope of article 5 (which sets out specific criteria[9] for the identification of OES's). whereas DSPs are any legal person providing an '[o]nline marketplace', an '[o]nline search engine' or a 'cloud computing service'.[10]

The security requirements for OESs are defined as follows in article 14 (1):

> 'Member States shall ensure that operators of essential services take **appropriate and proportionate technical and organizational measures** to manage the risks posed to the security of networks 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 networks and information systems appropriate to the risk presented**.' [emphasis added]

Article 16 (1) regulates the security requirements for DSPs, which are by and large similar (except for a few words that suggest a slightly more relaxed interpretation, which is also described in the recital).[11] It also includes a listing of elements to take into account when ensuring the appropriate level of security:

> "(a) **the security of systems and facilities**;
>
> (b) incident handling;

[8] See (in particular) recitals 3-7, as well as *Markopoulou et al. (2019)*, for a general overview.

[9] According to article 5, an entity can only be defined as an OES when it is providing 'a service which is essential for the maintenance of critical societal and/or economic activities' and where 'the provision of that service depends on network and information systems.' Furthermore, an incident would need to 'have significant disruptive effects on the provision of that service.'

[10] Articles 4 (4) and 5; article 4 (6) and (5), and annex III.

[11] See also recital 49.

(c) **business continuity management**;

(d) **monitoring, auditing and testing**;

(e) **compliance with international standards.**"

These security requirements are further expanded on in Commission Implementing Regulation (EU) 2018/151[12] article 2 (1), of which I will include the most relevant clause among those security elements a DSP is required to include:

> '(a) the systematic management of network and information systems, which means a mapping of information systems and the establishment of a set of appropriate policies on managing information security, including risk analysis, human resources, **security of operations**, **security architecture**, **secure data** and system life cycle management and **where applicable, encryption and its management**'

2.2 Methodology

I have decided to use these four articles as the core elements of establishing a framework of regulatory requirements to organisations who process data digitally. While the GDPR deals with the processing of personal data, and the NIS Directive deals with digital services on a more general scale, the fact is that most organisations who use digital systems in their operations will somehow be required to comply with the levels of security outlined in these regulations (not least due to the fact that practically all organisations process personal data in some manner). This is why I have decided to use these frameworks as the foundation of my analysis: because they appear to be the most applicable regulation to comply with when attempting to decide on a level of security for digital operations in general, and the encryption of data they store or transfer in particular.

As we have seen from the sections quoted above, there are some striking similarities between the GDPR and the NIS Directive in regulating data security. Through the wording, it appears as if the EU has had a more or less clear intent in connecting these two frameworks within data security and IT security – even if, formally speaking, they can never fully be considered *the*

[12] 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.

same framework.[13] It is also worth noting that GDPR article 32 is by and large similar to DPD[14] article 17,[15] whereas GDPR article 5 is virtually the same as DPD article 6 (1).[16]

If we are to summarise the contents of the four abovementioned articles, we could give the following aggregated list of requirements to the organisation processing the data in question:

- The organisation in question must take
  - **Appropriate technical measures**
  - **Appropriate organisational measures**
- To ensure: **A level of security appropriate to the risk** (presented or posed to)
- Have regard to **the state of the art**

The GDPR includes regard taken to 'the costs of implementation' as well as 'the nature, scope, context and purposes of processing', while the NIS Directive also includes certain specific elements to take in mind. However, considering the overlapping wording, it is hard to see that any of these are mutually exclusive to the subject matter. On the contrary, they would seem to contribute to the basis of the framework, seeing how these are all relevant elements in the larger, discretionary risk assessment which the regulations call for.[17]

If we are to summarise these requirements further, an organisation must identify and understand what data it processes (personal or business/service data), either in transit to or from the organisation, or while being stored within the organisation.[18] Based on the critical or sensitive nature of the data, the data must have its confidentiality ensured (meaning only the organisation, and those within the organisation with a need to access the data, should have this access) in a

---

[13] See *Voigt and von dem Bussche (2017)*, p. 42 and Cédric Burton in *Kuner et al. (2020)*, p. 633. *Markopoulou et al. (2019)* gives an analysis of the GDPR and the NIS Directive, and they believe any assessment under the two frameworks to be mutually exclusive, so that any assessment must in writing take due regard to both regimes. However, the authors do not comment on the substantial contents of the requirements, which are the main subject of this thesis. See also *Høringsnotat om utkast til lov som gjennomfører NIS-direktivet i norsk rett (2018)*, p. 40-41, where reference is made to the corresponding guides on each of the frameworks from NCSC (UK) and their substantial similarities.

[14] *Directive 95/46/EC* of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive – DPD).

[15] The main difference concerns the responsibility of the processor, whereas the wording concerning the security level is largely the same, see Cédric Burton in *Kuner et al. (2020)*, p. 632.

[16] See Cécile de Terwangne in *Kuner et al. (2020)*, p. 312.

[17] Risk management is a vast and complex discipline, and such concepts are important when deciding on security measures. Encryption is only one of many elements in risk management, but obviously an important one. See also *Harris and Maymi (2018)*, chapter 1, for more on this topic.

[18] I will henceforth refer to the general category 'data processing', for both data storage ('data at rest') and data transmission ('data in transit').

proportionate manner.[19] This means that either set of regulations set out a definitive standard for technical or organisational measures, but requires a case-by-case approach based on the risk which lacking confidentiality might entail. However, this also lays the ground for sector-wide regulation, where appropriate.

It is also worth noting that encryption is only mentioned in the GDPR as one of many suggested security measures – meaning the wording does not seem to require the use of encryption for data processing to be secure. The NIS Directive itself makes no mention of the concepts at all, even though it is present in the implementation regulation.[20] A valid argument could therefore be that a minimum requirement for encryption of data processing is purely theoretical; there are in fact no requirements, only recommendations. As we will see below, however, there is ample evidence that hardly any data processing can be done through appropriate security measures without the application of encryption, and 'the state of the art' in data processing practically entails encryption.

The requirement that the level of security must consider 'the state of the art' is of particular importance to the methodology in this thesis. 'The state of the art' is not defined in the relevant regulation, but it is normally understood to be the latest proven and tested efficient technology readily available, meaning not necessarily the latest model, but the technology which independent experts might think is the most optimal choice for your security needs.[21]

This means that the case-by-case approach mentioned above must be supplemented by updated information on what level of security might be reasonably understood as sufficient for its intended use within the technology scene. Both regulations are intended to be technology neutral, and requires an assessment of appropriateness in comparison to other reasonable considerations to take in deciding a level of security.[22] As such, it is challenging to establish a de lege lata-reading of the regulation, as it will always require updated information on the state of the art within each security measure – effectively *future-proofing* the regulation. At the same time, there is no apparent authoritative source to this information and the level which is, in fact,

---

[19] The 'appropriateness' in the GDPR is considered an expression of the proportionality principle under EU law, see Cédric Burton in *Kuner et al. (2020)*, p. 635. It is reasonable to read this into the NIS Directive as well.

[20] *Commission Implementing Regulation (EU) 2018/151*. See chapter 2.1 regarding the relevant clause in article 2.

[21] The EDPB defines 'state of the art' as 'an obligation on controllers […] to take account of the current progress in technology that is available in the market. This means that controllers must have knowledge of and stay up to date on technological advances, how technology can present data protection risks to the processing operation, and how to implement the measures and safeguards that secure effective implementation of the principles and rights of data subjects in face of the technological landscape', see *EDPB (2019)*, with further references to the relevant German case law believed to have inspired the term. See also *CPDP (2020a)* for some remarks on the practical usage of the term.

[22] See Cédric Burton in *Kuner et al. 2020*, p. 636, on the GDPR. Again, the same would appear to be the case for the NIS Directive. See also *GDPR*, recital 15.

appropriate, in any given situation. The means to answer this question, and in turn, the research question, will therefore be the sources which may reasonably be considered sufficiently authoritative to shed light on the levels of encryption required for different types of data processing. One might therefore say that while the wording of the relevant regulation is *de lege lata*, the lack of specific guidance on understanding the contents, also introduce a *de lege feranda*-exercise.

The methodology I have decided to pursue is therefore as follows:

(i) Identify what sources are relevant to understanding the contents of the security requirements in the GDPR and the NIS Directive, and establish their importance in relation to each other.

(ii) Examine those sources for information they have on encryption, in particular what information and guidance are given on different technical designs.

(iii) Through this examination, draft an overview of what level of encryption might be considered appropriate, and if possible, why that is.

(iv) If it can be interpreted from the sources, what level of encryption might be considered secure at a higher level, e.g., for particularly sensitive data.

(v) Finally give an overview of what information is available to establish the mode of protection required under current regulation, and what shortcomings there may be.

I mentioned earlier how I would focus the thesis on the level of encryption required under Norwegian law. The GDPR is incorporated in Norwegian law through The Personal Data Act[23], section 1.[24] In case of antinomy, the act will have precedence.[25] When I refer to the GDPR throughout this thesis, it is to be understood interchangeably with The Personal Data Act under Norwegian law.

The NIS Directive is thus far not implemented into Norwegian law. However, being EEA-relevant, it has undergone the main stages of implementation, and interesting parties have submitted comments to the consultation document and the draft bill.[26] Reportedly, a proposition is

[23] Lov om behandling av personopplysninger (*personopplysningsloven*) [*The Personal Data Act*] (2018-06-15-38).

[24] See also Agreement on the European Economic Area (*The EEA Agreement*), article 7 (a).

[25] See Lov om gjennomføring i norsk rett av hoveddelen i avtale om Det europeiske økonomiske samarbeidsområde (EØS) m.v. (*EØS-loven*) [Act implementing the main part of the Agreement on the European Economic Area etc. into Norwegian law – *The EEA Act*] (1992-11-27-109), section 2 and *personopplysningsloven [The Personal Data Act]* section 2 (4).

[26] See *Høringsnotat om utkast til lov som gjennomfører NIS-direktivet i norsk rett (2018)* [Consultative paper on the draft bill implementing the NIS Directive in Norwegian law]. See also the corresponding report, *NOU 2018: 14*: 'IKT-sikkerhet i alle ledd' (Holte-utvalget) [The Holte Commission - Official Norwegian Report].

currently being prepared by the Department of Justice.[27] While a directive need not be implemented in the same manner as regulation under EU law, the consultation document suggests one may reasonably expect the NIS Directive to be incorporated in Norwegian law for all intents and purposes. When I refer to the NIS Directive in the thesis, it is to be understood as the NIS Directive as it is currently planned to be implemented under Norwegian law, to the best of my knowledge at the time of writing.

I will refer to the articles from the GDPR and the NIS Directive included in chapter 2.1 as the 'relevant regulation' throughout the thesis. Even though the relevant regulation must be understood under Norwegian law, there is good reason to believe the recommendations to be read from the thesis to be substantially transferable to other EU- or EEA-countries.

I will refer to *encryption* when I discuss the use of cryptography to ensure confidentiality, however, the underlying technology and the study of this will be referred to as *cryptography* where suitable.

2.3 Delimitation

To make it clear, I will only deal with one specific security measure under the security measures required under the relevant regulation, namely *encryption*. Pseudonymisation is mentioned together with encryption in article 32 GDPR, not because they ensure confidentiality to the data in a similar manner, but because they ensure the confidentiality of the *personal* data in question. Pseudonymisation only ensures that the identifying factors of the data are removed, whereas encryption ensures that the data in question may not be accessed by unauthorised persons. For this reason, I will not go into pseudonymisation in this thesis, nor any other similar security measures not considered encryption per the definition in the next chapter.

Hashing (or hash functions) deserves a special mention, as it is very often mistaken for encryption, when they are in fact only related technologies. Hash functions ensure the integrity of data and are commonly used for digital signatures. They are pivotal to secure computer systems but are more relevant for the integrity-side of the security triangle and are consequently outside of the scope of this thesis.[28]

Much academic interest has been offered the problem of governments controlling, limiting and even sabotaging encryption schemes – to ensure that law enforcement and intelligence agencies are given the necessary surveillance capabilities.[29] This problem was well-known back in the

[27] See *Meld. St. 5 (2020-2021)* [Report to the Storting – White Paper], pp. 85-86.

[28] See *Paar and Pelzl (2010)* p. 293.

[29] A general overview may be found in *Soesanto (2018)*.

so-called *crypto-wars* of the 1990s, and the Snowden revelations in 2013 made its relevance in our time abundantly clear.[30] While this aspect is highly relevant to the development and history of encryption, it goes beyond the scope of this thesis. Encryption recommendations in many countries are likely to be influenced by government interests and may possibly have influenced the recommendations I will discuss in this thesis. However, this aspect must be the examined by other researchers.

I have earlier made the distinction between *data in transit* and *data at rest*, which are important terms within computer security, and in particular the data protection, and which I – for the sake of simplicity - will refer to as *data processing* throughout the thesis. In the life cycle of data within an organisation, the obvious missing link here is *data in use* - because at some point in time it is inevitable that data will be accessed from a device, loaded into memory, through the electronic circuits connecting the memory to the central processing unit (CPU), and more often than not, further on into the graphics processing unit (GPU), and out to a human-machine interface, such as a screen and corresponding controls. When data is in use like this, it is incredibly difficult, almost impossible to encrypt – and quite impractical as a security measure. Instead, there are other measures one needs to apply to protect the data being accessed from malicious software, various security flaws and prying eyes – which will not be covered in this thesis.[31]

2.4 Overview of sources of relevance

I will here give a very brief overview of what sources are relevant when answering the research question set out in the introduction, and what weight should be given to the guidance found in them.

The obvious starting point when identifying sources for the interpretation of the relevant regulation in this thesis (beyond the wording, which is discussed above) are the goals set out in the GDPR and the NIS Directive. As with all regulation in EU law, this is key to understanding the scope of the regulation, and this is particularly true when open terms, such as 'appropriate' are used – these point towards the proportionality principle in EU law.[32] Of relevance to the research question is therefore the explicit goal in the GDPR to ensure the 'confidentiality of stored or transmitted personal data' from, inter alia, 'unauthorised access'.[33] The GDPR therefore has

[30] Both the crypto-wars and the Snowden revelations have been the subject of many books (both academic and popular), documentaries and even a biopic. For a very brief introduction on the crypto-wars, I would suggest to the interested reader the episode 'Crypto Wars' in the podcast *Darknet Diaries (2018)*, which gives a good summary. A relevant account on Edward Snowden's revelations can be found in *Greenwald (2014)*.

[31] *Harris and Maymi (2018)*, chapter 3, supplies an excellent overview of the threats present when data is in use – and possible measures to mitigate them.

[32] See e.g., *Harbo (2010)*, for a general overview of the proportionality principle under EU law.

[33] *GDPR*, recital 49.

a strict focus on the security of personal data and its processing. The NIS Directive, however, has a broader scope (the uninterrupted accessibility of the digital services supplied by an organisation) and sees network and information security as a means to avoid 'major damage to the economy of the Union' from security breaches (most likely towards OES's), but also for 'the smooth functioning of the internal market'.[34] The former goal appears primarily oriented towards the potential consequences of cyberattacks on OES's, whereas the latter is oriented towards the necessary harmonisation of DSP's and their security levels to ensure a functioning free market in a digital age.[35]

Certain other articles in the relevant regulation shed some light on the interpretation of the articles. GDPR article 25 requires *security by design* in the processing of personal data, translating to security measures being part of the design of the systems used, as early in the process as possible. A similar requirement is not present in the NIS Directive, without this necessarily implying anything. Both seem to stress the importance of establishing standards, to which anyone subject to the regulation may wish to comply with – which in turn would lead one to believe this also to imply compliance with the relevant regulation.[36] The Cybersecurity Act[37], albeit fairly new, seems to be a stepping stone in this scheme of certification. The recitals are also a valuable source of information in the interpretation of the relevant regulation.[38]

As the research question is asked from the perspective of Norwegian law, both the wording in the national legislation implementing the relevant regulation and its preparatory works are relevant sources. Related statutory law may also supply some guidance, for instance the Security Act[39] and its related regulations, as well as other authoritative governmental documents on information security in general and encryption in particular. In this regard, a significant corpus of committee reports, policy/strategy documents are relevant, as well as expert advice guides from both the national security authorities[40] and the Norwegian DPA[41]. Case law will also be relevant, where available.

---

[34] *NIS Directive*, recital 2-3.

[35] *NIS Directive*, recital 5.

[36] See, inter alia, *GDPR*, article 40, on the establishing of codes of conduct, and the *NIS Directive* article 11, on the 'cooperation group', and article 19, on standardisation.

[37] *Regulation (EU) 2019/881* of the European Parliament and of the Council of 17 April 2019.

[38] See e.g., *Baratta (2014)*, p. 296-297 (with further references), attributing recitals with a 'supplementary normative nature'.

[39] Lov om nasjonal sikkerhet (*sikkerhetsloven*) [*Act on National Security / The Security Act*] (1998-03-20-10). The Norwegian National Security Authorities have made a significant effort in providing ease of access to its contents through specific guides, see e.g., *NSM (2020a)*.

[40] The Norwegian National Security Authority [Norsk Sikkerhetsmyndighet] - NSM. Datatilsynet (The Norwegian DPA) also links to their guides, see e.g., *Datatilsynet (2017)*.

[41] Case law from all DPAs will be relevant, see below, but decisions from the Norwegian DPA will carry more weight from a Norwegian perspective, due to their availability.

On a European level, guidelines and recommendations from the European Data Protection Board (EDPB), the European Union Agency for Cybersecurity (ENISA)[42], and the NIS Cooperation Group[43] are of particular relevance, as well as any CJEU case law which might touch on the topic. Case law from national DPAs may be of interest, unfortunately there is not much case law outside of English-speaking countries available in English. Guidance and recommendations from other DPAs are also relevant sources, again, pending their language availability. This also applies to national (cyber-)security authorities.

Even though European standards are scarce, many relevant, comparable standards are available. They may be of interest, particularly if they are referenced by any of the bodies mentioned above (this would give them an authoritative edge). To the level the underlying regulation is comparable, case law outside EU may give some guidance, for instance from the Federal Trade Commission (FTC) in the US.

Finally, legal literature does carry some weight, in particular when some of the relevant regulation is fairly new. And last, but not least, technical literature is duly pointed at to establish 'the state of the art', and will need to be taken into account as far as it sheds light on the legal requirements in the research question.

3 A very brief introduction to cryptography and encryption

3.1 Overview

Encryption is by the Information Commissioner's Office (ICO), the UK DPA, defined as 'a mathematical function that encodes data in such a way that only authorised users can access it'.[44] The goal is to allow a message or another type of information to be unreadable to anyone but those intended to access it. It works by way of a cryptographic technique or algorithm (often called a *cipher*), and a *key* (a secret value, of a certain length – and correspondingly – strength, the *key size*)[45], which transforms *plaintext* (information which can be read and accessed) into *ciphertext* (information which is incomprehensible).[46] It is an essential part of modern data security and lies at the core of the *confidentiality* principle in data processing. It is also a specific way to demonstrate compliance with this principle, in whichever form it may be set out in

[42] Formerly the *European Network and Information Security Agency*, hence the abbreviation.

[43] Established under the *NIS Directive*, article 11.

[44] *ICO (2019a)*, p. 236-237.

[45] It should be noted, though, that key sizes cannot be *compared* between ciphers as a measure of strength, as they utilise key sizes differently, cf. *Aumasson (2018)*, ch. 3.

[46] *Datatilsynet [The Norwegian DPA] (2020)*; *Aumasson (2018)*, ch. 1.

regulation.[47] In this short chapter, I will attempt to give a brief overview of encryption, why it is used, and how it is ideally applied. Hopefully, this technical introduction will make the next chapters easier to understand.

Encryption only relates to the process of converting plaintext into ciphertext, whereas the science of doing this is known as *cryptography* (or sometimes *cryptology*). Simple methods of encrypting messages go far back but has only become the advanced techniques that we know today through the processing of data by way of computers. A cipher works with two components: the *permutation* is a function that transforms an item (for data, a group of *bits*) such that each item has a unique inverse, whereas the *mode of operation* is an algorithm that uses a permutation to process messages of arbitrary size. The permutation uses a key to complete the transformation – this is important, as only someone with the key should be able to reverse the operation to access and read the plaintext. Finally, the resulting ciphertext should look *random*, meaning that it should be impossible to find a pattern or other method to reverse the operation without the key.[48]

In cryptography, a cipher is considered secure 'if, even given a large number of plaintext-ciphertext pairs, nothing can be learned about the cipher's behavior when applied to other plaintexts or ciphertexts.' The main measure for this is *attack models*, which are assumptions about what the attacker can and cannot do, and *security goals*, which is what a successful attack would achieve. Combined, we are particularly interested in the *security notion*, which is under what circumstances an attacker will be unable to reach his security goal – in which case the ciphertext remains hidden and protected.[49]

These are some of the key concepts to keep in mind when comparing and assessing encryption methods. Simply put, whenever someone develops cryptographic measures to keep information of interest hidden, there will always be someone who is working to break the cipher and access the plaintext. Sometimes the attacker will be someone with an interest in the data itself, and sometimes the ability to break the cipher will be the main goal – and these interests do not seldom overlap. Other times the attacker will want to break the cipher to prove its ineffectiveness, for instance to encourage the research in, and use of, improved cryptographic methods. This leaves a constant technological battle, where there is a continuous need for the users to keep up with the latest development – if they want to keep their ciphertext secure.

[47] *ICO (2019a)*, p. 236-237.
[48] *Aumasson (2018)*, ch. 1.
[49] *Aumasson (2018)*, ch. 1.

3.2 Encryption and digital data

Encryption today is almost exclusively performed by computers, and they utilise such advanced algorithms that they would take enormous time and manpower to be performed by humans. This is important to keep in mind when we are to assess (or rather, assess the assessments of) the security which cryptographic algorithms supply: at its core, all these algorithms are instructions performed by computers. Being the logical units they are, computers are inherently *predictable*, which is why all ciphers eventually are broken (at least history has shown this so far). To 'trick' computers from finding patterns and similarities in the ciphertext (often referred to as *collisions*), clever efforts must be made to make the ciphertext look as random as possible, so called *randomisation*. The problem is that *true randomisation* does not exist for computers, as they are only able to follow instructions and have no 'free will'. Ciphers mitigate this by pseudo-randomisation, which makes the resulting ciphertext look as random as possible. The details of the inner workings of common ciphers and how they may be attacked go beyond this thesis.[50]

In short, any ciphertext produced by a computer, will most likely be possible to break by a computer with sufficient computing power. This is referred to as *cryptoanalysis*.[51] On average, computing power doubles over the course of 18 months, and a cipher should therefore be designed to withstand the attacks it may be exposed to within (at least) the estimated data life cycle[52] of the plaintext. When we assess a cipher, we must therefore have regard to the data it is meant to protect. We must also keep in mind that there is always a chance for collision through cryptoanalysis, not least due to the fact that most ciphers are known and have often had both their source code published and been audited.[53] Also, the more ciphertext available with a certain key, the easier it is to break. And when a cipher has been broken, whoever breaks it might not find it in their interest to inform the general public – they may wish to keep that

[50] *Aumasson (2018)*, ch. 1. See also the remaining chapters for more insight in how modern encryption works, and previous, existing, and future challenges.

[51] See *NOU 2015:13*, p. 57.

[52] The *data life cycle* (or *information life cycle*), refers to how a set of data moves through the computer systems of an organisation, sometimes being processed (having data added, changed or removed) and sometimes simply staying put, waiting to be useful. Understanding the life cycle of an organisation's data is vital to addressing its security needs, see *Harris and Maymi (2018)*, ch. 2.

[53] This might seem counterintuitive, but the consensus is both that encryption needs to be understood to be adopted, and that transparency is necessary to avoid back doors – which have traditionally been abundant. See *Aumasson (2018)*, ch 3, and note how practically all ciphers discussed there (also throughout the other chapters), are freely available to be tested. See also the previous references regarding the crypto-wars and the Snowden revelations (see chapter 2.3).

exploit (the term used for a security flaw)[54] for their own sinister uses. Finally, there is always the danger of human error: Any cryptographic algorithm fails if it is improperly used.[55]

Encryption is today used in a wide variety of uses, such as banking, online shopping, messaging, web browsing, personal data processing, video and voice calls, as well as various types of critical infrastructure operations. Among these, there are many types of encryption in use, and deciding the right one is not solely a question of appropriate security for its purpose, but also a question of the hardware requirements in place, what media is used for the data and the speeds required for efficient processing. Also, beyond choosing the right algorithm, it is important to choose the right key size, the right software, and to keep the key secure.[56]

The processing of data can, as mentioned earlier, roughly be divided into data at rest and data in transit, and these in turn have led to the two primary categories of encryption: symmetric and asymmetric encryption.

3.3 Symmetric encryption

This is what is normally thought of as encryption: encrypting plaintext with a key into ciphertext which can both be stored and transmitted, but will remain incomprehensible until someone with the same key uses it to decrypt the ciphertext into plaintext. Depending on the data life cycle, and the needs to access the data, very strong encryption may be used through symmetric encryption, and the data will be secure as long as the key remains secure. For obvious reasons, a secure key should always be kept in another place than the ciphertext itself, ensuring the confidentiality, availability, and the integrity of the key as well. If the key is lost, so is the data.[57]

Symmetric encryption is today mainly relevant with the storage of data on cloud services and data centres, but also physical storage on laptops, tablets, and phones, and even backups made on tape media or optical discs. Symmetrical encryption may also be useful when specific types of data is transmitted, where the recipient either already has the key, or has had it transferred to her by way of an alternative, secure communications method.[58]

---

[54] *CFCS (2020a)* defines 'exploit' as a code or method to exploit a software vulnerability (or lacking configuration) to cause a security incident.

[55] *Aumasson (2018)*, ch. 1.

[56] *ICO (2019a)*, p. 236-237.

[57] See *NOU 2015:13*, pp. 37-38, and *ICO (2019a)*, p. 236-237.

[58] Technically speaking, this might be considered data in transit, but for effective encryption purposes, it should still be considered data at rest, because the encryption method is independent of the transmission method.

While symmetric encryption may seem 'conventional', significant research is done within its applications. The most relevant technological advances in this area is *fully homomorphic encryption* (FHE). The goal of this technology is to allow modifications to the data in real time with no need to decrypt the data, for instance by modifying the individual entries in the database or the cells in a spreadsheet without accessing the rest of the document. This is likely to improve security of cloud services significantly, but there remains work on this technology before it can reach its full potential.[59]

3.4 Asymmetric encryption

The problem with symmetric encryption as a means for secure communications is the fact that the key must be known by both parties, effectively limiting this type of communication to cases where both parties have met or otherwise exchanged keys (often referred to as the *key distribution problem*).[60] This is solved with asymmetric encryption, in which different keys are used for encryption and decryption, and these are interconnected through advanced mathematical functions. This ensures what is known as *end-to-end encryption*, or *public-key cryptography* (due to the use of a 'public' key and 'private' key). The concept of asymmetric encryption may seem simple, but the inner workings are not, which is why this must be referred to the technical literature.[61]

What should be noted, is that asymmetric encryption pays an important part in most encryption of data in transit, very often combined with other technologies (such as symmetric encryption, hashing, and digital signatures). Most of our online communication (and which, correspondingly, organisations conducting parts of their business through online services has to deal with) uses public-key cryptography through *digital certificates*. This is a method by which two computers, typically a user and a web site, will set up secure communication through a certificate from a trusted third party (a *certificate authority*) and in turn, keys generated through the certificate. When this method is properly implemented, it ensures that no one but the two parties communicating are able to decrypt the communication – they are the only one with the keys.[62]

3.5 The future of quantum computers

No technical introduction to cryptography would be complete without a mention of the long-anticipated advent of *quantum computers*. Simply put, these are computers, which in theory,

---

[59] *NOU 2015: 13*, p. 51. See also *Aumasson (2018)*, ch. 1.

[60] *Paar (2010)*, p. 150.

[61] See *Aumasson (2018)*, ch. 10-13.

[62] See *NOU 2015: 13*, p. 37-38 and *ICO (2019a)*, p. 236-237.

can achieve performance which far surpasses the technology available today, and the possible limits of conventional computers. This makes ciphers that today may be considered secure for the foreseeable future, possibly broken with the introduction of quantum computers, not due to flaws or bugs, but due to sheer computing power.[63]

For this reason, future-proofing ciphers beyond the age of quantum computers requires extremely strong ciphers. How strong they need to be to achieve this is hard to say for certain, but experts currently believe that today's strongest symmetric encryption methods may withstand the computing powers of quantum computers, whereas today's strongest asymmetric ciphers will be broken.[64]

3.6 The state of the art in cryptographic algorithms

This chapter has a dual purpose: not only to give a technical introduction, but also to introduce what might reasonably be considered state of the art within the technical literature. As presented in the methodology section, the term introduces a review and overview of the technical debate on the issue, which implies that to interpret the law, one must also seek the advice of the experts in the literature. This must at least be true when there is a lack sufficient authoritative sources on the subject, and also if these sources are dated (which may often be the case).[65] Even if guidance is available, it must still be assessed if this fully reaches the requirement of the state of the art, or if there are more questions to asked and answered.

This chapter must therefore always be kept in mind when reviewing the guidance and security levels suggested in the next chapter. Where any of the sources in the next chapter supply limited information, one is to confer with this chapter and the sources mentioned here to reach the technical insight needed to assess the state of the art, and whether a given solution is appropriate when this regard is taken.[66]

---

[63] *NOU 2015: 13*, p. 51. See also *Aumasson (2018)*, ch. 14.

[64] *Aumasson (2018)*, ch. 14.

[65] In my research, I have noted that both DPAs and cybersecurity agencies struggle to supply updated information, at least on a more detailed level. Understandably so, considering the research needed to keep this information up to date and relevant.

[66] *Aumasson (2018)* seems to be one of the most updated textbooks in the area, and each chapter contains references to further reading on the subject. The ciphers discussed also have their strengths and weaknesses evaluated, as they appear at the time of writing.

4 Cryptographical requirements for organisations

4.1 To encrypt, or not to encrypt

Having outlined the technical capabilities (and limitations) of current and available encryption methods in the previous chapter, we have a fair understanding of how one might assess the 'state of the art' in cryptography. Not that any interpreter of the law may reasonably have full insight into this, but at least to the level seemingly intended in the relevant regulation.

The relevant regulation, however, does not explicitly require encryption of data, neither the personal data of the GDPR or the service-critical data of the NIS Directive. As discussed, encryption is only suggested as one of many security mechanisms in the GDPR and is not even mentioned in the NIS Directive. Which leads us to a necessary question:

> *Does the relevant regulation require the use of encryption for the security level to be appropriate? And if so, is it a general rule?*

The reason I pose the question in this manner, is the underlying proportionality principle in the assessment of 'appropriate'.[67] This might simply refer the question to a case-by-case approach, where security must be weighed against all other parameters. In my opinion, the question of encryption is an all too important element in information security to be answered with 'it depends'. There are numerous sources giving more or less direct guidance on whether encryption generally should be used, and we will review these in the following.

The intelligence communities and other authorities responsible for the national security have always been the prime mover in the development and application of encryption. It should therefore come as no surprise that the Norwegian Security Act requires all government authorities to use encryption when processing sensitive information. This also applies to anyone contracted to supplying services for these purposes.[68]

Beyond this, there is little hard law on the subject in Norway, with one noteworthy exception: The Personal Health Data Filing System Act of 2014.[69] Section 21 of the act refers to GDPR article 32, and not only suggests, but *requires* the use of encryption for health data containing personal data under sections 10 and 11. At the time of writing, these seem to be the only cases

[67] See 2.2 above.

[68] *Sikkerhetsloven [Act on National Security / The Security Act]*, sect. 5-6, cfr. sect. 1-2.

[69] Lov om helseregistre og behandling av helseopplysninger (*helseregisterloven*) [*Personal Health Data Filing System Act*] (2014-06-20-43). The relevant section was revised in 2018, with the implementation of the GDPR.

in Norway where hard law requires the use of encryption, which although limited in scope, does give an indication on the Norwegian government's position on the use of encryption.

The Norwegian Government has also made it very clear that it does not only encourage the use of encryption for the government administration and related offices, but also to the general public and, in particular, private businesses.[70] Online communication is specifically mentioned as a type of communication which *should* be encrypted, no matter if the server is public or private.[71] However, the government is careful not to impose the use of encryption as a general rule, and refers to encryption as one measure which *might* ensure information security.[72]

The Norwegian DPA does not give any particular guidance on the question, but refers to the National Security Authority (NSM).[73] Interestingly, NSM goes much further than the previously mentioned recommendations, calling encryption a 'prerequisite for the security of information and communication systems'.[74] On the other hand, the British counterpart to NSM, the National Cybersecurity Centre (NCSC) again only refers to encryption as an 'example' of a security measure.[75]

ICO (the British DPA) refers to the 'widespread availability and relatively low cost of implementation' of encryption and recommends encryption for all activities when personal data is stored or transmitted. The standard most often referred to by relevant authorities, ISO 27001:2013, seems clear in the section on 'Communications security' that cryptographic techniques should be applied to comply with the standard.[76]

While it seems that the jury might be out on the question of there being a general rule on the use of encryption to comply with the relevant regulation, it is worth noting that the most recent recommendation – from the National Security Authority – goes one step further in suggesting that encryption should be present for an information and communication system to be secure.[77] This is also the institution at the forefront of such questions under Norwegian law, and it would therefore seem fair to say that the state of the art in security for data at rest and data in transit

---

[70] *Norsk kryptopolitikk [Norwegian Encryption Policy] (Policy Paper, 2019)*, pp. 15-16.

[71] *NOU 2015: 13*, p. 308, which references the recommendations in *NSM (2015)*, pp. 41-42.

[72] *Norsk kryptopolitikk [Norwegian Encryption Policy] (2019)*, p. 20; *NOU 2015: 13*, p. 41.

[73] *Datatilsynet [The Norwegian DPA] (2018a)*; *(2019a)*.

[74] *NSM (2020b)*, p. 32 (my translation).

[75] *NCSC (2018)*, p. 8.

[76] See section A.13.2.1 on 'Information Transfer Policies and Procedures'. See also *Chopra and Chaudhary (2020)*, p. 184-185.

ISO 27001:2013 is referred to in, inter alia, *NSM (2020b)* and *Datatilsynet (DK) [The Danish DPA] (2018)*.

[77] See *NSM (2020b)*, p. 32 and previous footnote.

implies the use of encryption in all cases where information of any value to anyone is stored or transmitted, and this is possible through practical means.

4.2 General guidance on the use of encryption

If we consider it a reasonable notion[78] that encryption in general *should* be used when data is processed under the relevant regulation, it is necessary to address the question of what *type* of encryption should be used and how it should be *applied* to be in compliance. As we saw in chapter 3, cryptography is an advanced science, and it is a considerable challenge to understand which cryptographic technique will give the appropriate security level. I will start this section by looking at what can be said about encryption on a general level, and then go on to the particular types of encryption relevant and recommended for data at rest and data in transit.

The Norwegian government is reserved in its general recommendation in types of encryption but refers to international established standards and approved NATO-standards for guidance. In particular, they refer to the US *National Institute of Standards and Technology* (NIST) and their updated standards. Further, the *NATO Communication and Information Systems Security Standards (CIS3) C&I partnership* is mentioned, due to the cooperation with their own NSM. I will revert to some of these standards towards the end of the chapter, as they lead us into a level of abstraction which is more relevant to specialist needs.[79]

4.2.1 High-level recommendations

NSM continuously updates one very essential document: *NSM Cryptographic Recommendations*.[80] This is the minimum requirements for cryptographic techniques for information handled by the government or its contractors under the Security Act, and can therefore be considered a *state of the art*-recommendation for information security needs at the highest level.[81] This is helpful, as it allows us to estimate a security level which under all normal circumstances should be considered appropriate, and in fact should be sufficient even for more sensitive information. It is more specific in its recommendation than other types of guidance, while avoiding the detailed accounts of the standards often referred to (but referring to them, and seemingly incorporating parts of them). I will include the most relevant and specific recommendations here:

[78] From the preceding chapter, we cannot definitely conclude on encryption as being required under a general rule, it will nevertheless be necessary with specific assessment of the processing at hand. While there will be many cases under the relevant regulation where encryption is not (necessarily) an appropriate measure, these are of limited interest to the research question, and generally fall outside the scope of this thesis.

[79] *Norsk kryptopolitikk (2019)*, p. 21.

[80] *NSM (2020c)*.

[81] *NSM (2020c)*, p. 1.

- *Professional advice* should always be sought before implementing cryptographic techniques.[82]
- All cryptographic techniques applied should use *unpredictable secret and private keys* (see chapter 3.2, on the subject of randomisation).[83]
- **Symmetric cryptography** should use
    - Advanced Encryption Standard (AES)[84]
    - with a key length of *at least 256 bits*[85]
    - with one of the following modes of operation:[86]
        - *Counter-mode (CTR)*
        - *Cipher-block-chaining (CBC)*
        - *XEX Tweakable Block Cipher with Ciphertext Stealing (XTS-AES)*
    - with one of the following message authentication codes (MAC):[87]
        - *Cipher-based MAC*
        - *Hash-based MAC*
    - with one of the following authenticated encryption modes:[88]
        - *AES Galois Counter Mode (AES-GCM)*
        - *Counter with CBC-MAC (CCM)*
    - with one of the following key wrap functions:[89]
        - *AES Key Wrap (KW)*
        - *AES Key Wrap with Padding (KWP)*
    - and the key derivation function:[90]
        - *Extract-then-expand*
- **Asymmetric cryptography** should use
    - Rivest–Shamir–Adleman (RSA)[91]
        - *Minimum 3072-bit modulus* (key strength)[92]

---

[82] *NSM (2020c)*, p. 1.

[83] *NSM (2020c)*, p. 2. See also further guidance on key management, which goes beyond the research question.

[84] *NSM (2020c)*, p. 3. AES is defined in *FIPS (2001)*.

[85] *NSM (2020c)*, p. 3.

[86] *NSM (2020c)*, p. 4. See also chapter 3.1, concerning modes of operation.

[87] *NSM (2020c)*, p. 4. Even though MACs are generally relevant to ensure the authenticity of the encrypted messages, I have included it due to its part in the AES cipher.

[88] *NSM (2020c)*, p. 5.

[89] *NSM (2020c)*, p. 5. Key wrap functions protect the confidentiality and integrity of cryptographic keys.

[90] NSM (2020c), p. 5. This ensures sufficient randomisation and unpredictability of the keys used.

[91] *NSM (2020c)*, p. 6. NSM does not seem entirely specific on recommending only RSA, rather suggesting it due to the strength in its method, and being open to a similar technique if it should be relevant and equally strong, see specific detailed guidance in 7.1 and 7.2 on p. 6.

[92] *NSM (2020c)*, p. 12.

- One of the following asymmetric signature algorithms:[93]
  - *Digital Signature Algorithm (DSA)*
  - *Elliptic Curve Digital Signature Algorithm (ECDSA)*
  - *RSA Signature Scheme with Appendix-Probabilistic Signature Scheme (RSASSA-PSS)*
- One of the following key exchange algorithms:[94]
  - *Diffie-Hellman Key Exchange (DH)*
  - *Elliptic Curve Diffie Hellman Key Exchange (ECDH)*

In addition, the guidance gives some recommendations on the mathematical functions needed for asymmetric cryptography, as well as further detailed recommendations on usage (for instance the generation of random numbers) and references to relevant standards.

It is important to stress that these are *high-level security recommendations*, which may supersede the needs for many, if not most, organisations to attain an appropriate security level. Conversely, certain organisations, processing particularly sensitive data, may even need to pursue more technical details and an even higher level of encryption (see below under chapter 4.6). Indeed, NSM does in fact mention quantum computing and certain considerations needed to future-proof data in these regards.[95]

4.2.2 Medium-level recommendations

Having reviewed the level of security recommended by the NSM, the question becomes what can be said about recommendations given which supply us with a *reasonable level of encryption security*. The Norwegian DPA generally refers these questions to the NSM and its guidance (which effectively comprises the beforementioned high-level recommendations), but does also supply some general advice:[96]

- Recognised ciphers and modes of operations should be used.[97]
- Symmetric cryptography: AES at 128- or 256-bit key length.
- Asymmetric cryptography: RSA with modules and secret exponents of at least 3072 bits.

---

[93] *NSM (2020c)*, p. 9.

[94] *NSM (2020c)*, p. 10.

[95] *NSM (2020c)*, p. 7-8.

[96] *Datatilsynet [The Norwegian DPA] (2017)*. There is also some guidance on key management, but this relates to the type of encryption (at rest or in transit), so will be discussed below.

[97] This might imply the known criteria 'state of the art', but it may also be a general caution on how well developed and audited a cipher is – reflecting on the general advice in literature on cryptography to stay away from lesser known and insufficiently tested ciphers (see *Aumasson (2018)*, ch. 1).

- Certified key management modules, such as Common Criteria[98] or FIPS 140-2[99] (see below under chapter 4.6 on standards).

The Norwegian DPA also points out the relation between cryptographic techniques and the systematic implementation of this in software development (privacy by design). The level of security needs to be the same throughout the software and the systems to be used, as shortcomings in one element will negatively impact the rest of the system (the weakest link in the chain, practically speaking).[100]

The French DPA, Commission Nationale Informatique & Libertés (CNIL), has also published a detailed guidance on encryption, which largely follows the same lines as NSM and the Norwegian DPA, although with some specific deviations:[101]

- Symmetric encryption: AES or AES-CBC with at least 128 bits key length.
- Asymmetric encryption: RSA-OAEP[102] with modules and secret exponents of at least 2048 bits, and RSA-SSA-PSS[103] for signatures.

Interestingly, CNIL also supply recommendations on what methods which specifically should *not* be used, due to being insecure, namely DES (Data Encryption Standard) and its derivative 3DES. It also points out certain other pitfalls, like confusing hashing for encryption (which is insufficient to protect confidentiality at the same level). Furthermore, it does provide specific recommendations to certain types of recommended software, which I will revert to.[104]

European DPAs have different approaches to how detailed guidance they provide. While the Norwegian DPA (through NSM) and the French CNIL give specific recommendations on ciphers and methods, the ICO attempts a more general approach, pointing out the importance in 'choosing the right algorithm, choosing the right key size, choosing the right software, and keeping the key secure.' Furthermore, a continuous assessment is needed to ensure the

[98] The Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408).

[99] FIPS 140-2 has since been succeeded by *FIPS 140-3 (2019)*, and I will use the latter as reference, even though many recommendations refer to the former (FIPS seems clear in its guidance always to use the latest recommendations).

[100] *Datatilsynet [The Norwegian DPA] (2019b)*.

[101] *CNIL (2018)*, p. 23.

[102] As defined in *RSA Laboratories (1999)*.

[103] As defined in *RSA Laboratories (1999)*.

[104] It also follows suit with Datatilsynet [The Norwegian DPA] in recommending the solutions certified or qualified by *Agence nationale de la sécurité des systèmes d'information* (ANSSI) [National Cybersecurity Agency of France], which is the French counterpart to NSM, see footnote 73.

cryptographic techniques are appropriate, and any type of sector-specific recommendation which may be relevant, should be taken in regard.[105]

Both NSM and the ICO point out the importance of establishing a strategy for the use of cryptographic methods, in effect ensuring a data protection by design-approach also when implementing new systems in an organisation. This is an important point, because as discussed earlier, the security level of combined and integrated systems is only as high as the lowest common denominator. They also both stress the importance of using encryption capabilities, where they exist.[106]

The title of this chapter is 'medium-level recommendations', and even though there may likely be recommendations out there for a lower security level which might be considered appropriate for certain types of data processing under the relevant regulation, they are likely not easier to implement, and most certainly broken (or will soon be) to the level where there would be little or no future-proofing. My research therefore suggests that the level of security the recommendations in this chapter gives, should be the lowest one seeks to implement, especially considering the authoritative sources giving weight to the recommendations.

With these general recommendations on encryption as a foundation, we will now have a look at what is recommended for the specific types of encryption related to the research question.

4.3 Guidance on data at rest

Data at rest, as the name implies, has to do with data which is stored on a type of hardware (computers, laptops, phones, etc.), on a type of storage facility (file servers, cloud storage etc.), or on any type of archival storage media (optical discs, archival tapes, etc.).[107] In general, this type of data is easier to protect than data in transit, because it should only be available to authorised users. However, this simplicity, and the enormous size some of these data collections may have, makes sloppiness and lack of control possible, and leaves encryption as an important failsafe.

Under today's data storage realities, we might roughly divide the protection of data at rest into two subcategories: own devices and cloud services. Cloud services, however, are something of a hybrid, as they by their nature comprise both data at rest and data in transit – and therefore

[105] *ICO (2019)*, p. 236-237. To be fair, the ICO also points out standards such as FIPS 140-2 and FIPS 197, and solutions from the NCSC, but this seems to be more of reference point, perhaps as a type of high-level recommendation.

[106] *ICO (2019)*, pp. 236-237; *NSM (2020b)*, p. 32.

[107] *NCSC (2019b).*

are subject to both sets of recommendations. I will therefore discuss the recommendations which deal with these in particular, in chapter 4.5.

In this segment, we will primarily consider data at rest on the organisation's own equipment. This comprises all types of devices controlled by the organisation (as well as employees' private devices set up to comply with the organisation's control mechanisms), and any other types of physical storage of digital data on premises controlled by the organisation. The data stored in such manners may constitute a significant security risk if stolen or lost, which is why *all data on such devices should always be encrypted*.[108] Failing to ensure this not only leaves the data important to your organisation at great risk, but will most likely be a breach of the relevant regulation, and has already led to large fines being issued under the GDPR.[109]

While most sources agree on encrypting data at rest on an organisation's own equipment, there seems to be limited information on *how* this should be done. Both NSM and ICO advises the use of *full disk encryption*, which means that data on the computer is encrypted in such a manner that a password must be input on start-up, and without this, all parts of the computer remains encrypted.[110] Alternatively, specific drives can be encrypted, so that sensitive data is not automatically available on computer start-up, but only after the correct password is input.[111] Data can also be encrypted inside the application processing a specific type of file[112], or a file or group can be encrypted, typically into a container. CNIL specifically mentions Veracrypt as a recommended method to do the latter.[113] The Norwegian DPA also lists a number of examples of encryption methods, at both the software and hardware level, and also at the operative system level (which is the recommended tool for full disk encryption), but always pointing to the underlying cryptographic technique as the deciding factor in choosing a method.[114]

---

[108] *NSM (2020b)*, p. 32; *NOU 2018: 14*, p. 119-120; *ICO (2019b)*, p. 10-13; *NCSC (2018)*.

[109] See *EDPB (2020)* for the case which the Danish DPA brought against the Danish municipalities of Gladsaxe and Hørsholm, where computers with personal data were stolen or lost, and none of the computers had their data encrypted. The DPA suggested fines of respectively DKK 100.000 and DKK 50.000.

[110] *ICO (2019a)*, pp. 236-237; *NOU (2018)*, pp. 119-120. NSM also used the term 'secure start-up' [sikker oppstart], because the lock needs to be surpassed on start-up. The hard drive could of course be physically removed from the computer and accessed from a different computer, but strong encryption would still make accessing the data unfeasible.

[111] *NOU (2018)*, pp. 119-120; *ENISA (2017a)*; *ENISA (2017b)*, p. 62.

[112] See *ICO (2019b)*, p. 12. For example, this document is processed in a word processor with the ability to use the encryption capabilities in the docx-format on this document, if needed. As always, one must consider the strength of the encryption when deciding if this (or any other) method should be used.

[113] *CNIL (2018)*, p. 23. Veracrypt, formerly Truecrypt, is the most popular open source project to enable file or disk encryption through containers. CNIL's recommendation might go beyond the fact that Veracrypt is maintained by a French team of developers; Veracrypt is also believed to be uncompromised by the backdoors thought to exist in many commercial solutions. (See *Leyden (2017)* for an overview of this debate.)

[114] *Datatilsynet (2017).*

One proposal from ENISA is noteworthy, which is specifically mentioned towards its 'high-risk level'-recommendations. This has to do with database level encryption, also called *searchable encryption*. They do not define the methods precisely, but from the context it seems clear that it is FHE[115] which is referred to and recommended for sensitive data.[116]

To summarise, all of the sources which I have researched are careful to avoid advising any one solution to the public, instead underscoring the cipher and its correct usage as the relevant parameter, and effectively referring us to the recommendations within symmetric cryptography (which is the obvious method to encrypt data at rest), and the state of the art within those techniques.

4.4 Guidance on data in transit

Data in transit is understood as data packages going from one terminal connected to a network (commonly the internet), to another terminal connected to the network. The internet allows an enormous number of terminals connected to the same network to communicate with another over the same physical lines by dividing the data into small *packets*, with data encapsulated in many types of metadata allowing for the vast amount of simultaneous communication links to co-exist seamlessly, and in most cases, with no interference noticeable to the users of the communicating terminals. The communication on these links may be e-mails, voice or video calls, online gaming, audio or video streaming, file transfers, or simply old-fashioned internet browsing.

The wide variety of communication makes the question of encryption challenging, as there are different reasons to keep these types of data secure. Clearly, person-to-person communication (e.g., e-mail, video or voice calls) or internet browsing is usually more sensitive data for most people than what show is currently being binged on Netflix, or who the opponents in the present game of Fortnite are. However, when encryption is so readily available, one might argue that there is no reason to leave any type of communication unencrypted. And at the very least, the users should be duly informed about what security measures are in place for different types of services and applications, to help them decide on an appropriate security level.[117]

4.4.1 Internet browsing

Internet browsing traditionally had little or no encryption enabled, except for banking services. This was the case in the 1990s and well into the 2000s, but the situation today is radically

[115] Fully Homomorphic Encryption (see above under chapter 3.3).

[116] *ENISA (2017b)*, pp. 65-66.

[117] See *Directive 2002/58/EC*, rec. 20.

different, with hardly any modern web site not allowing secure, encrypted communications, and many of them simply not allowing connections over unencrypted protocols at all. The standards and application capabilities are also on a very different level, with significant resources being spent on developing secure communication methods. For this reason, recommendations and guidance from trusted bodies are plentiful and detailed. In general, the following advice can be inferred:

- Client terminals should always ensure the web site they visit are encrypted over HTTPS[118] and web site owners should ensure their entire web site is running at HTTPS.[119] HTTPS uses certificate authorities (CAs) to generate key pairs to allow for end-to-end security (see above in chapter 3.4).
- HTTPS can use different encryption methods, notably SSL and TLS. SSL is outdated and should not be used.[120]
- TLS was recently released in version 1.3, which is recommended. Version 1.2 is still considered secure but will eventually be outdated.[121]
- Using (reasonably) available means, web site owners should test if their setup is vulnerable to penetration testing.[122]
- Lookups in the Domain Name System (DNS) should also be done securely and according to updated standards.[123]

The implementation of TLS is also described at length in several recommendations from NSM[124], ICO[125], CFCS[126] and NCSC[127] – to mention but a few. These recommendations are of such a technical nature that I will not discuss them further, but they are a valuable point of departure to anyone working with securing online systems. As always with such recommendations, regard must be taken to how recently they have been published (or updated), and any technical developments of importance having taken place since.

---

[118] HTTPS is the secure version of the ordinary internet communications protocol HTTP (Hypertext Transfer Protocol). The 'S' is short for Secure.

[119] *ICO (2019b)*, pp. 15-16; *Digitaliseringsdirektoratet [The Norwegian Digitalisation Agency] (2020)*; *ENISA (2017a)*.

[120] *Datatilsynet (2017)*; *ICO (2019b)*, p. 15-16. The agencies are not unanimous on SSL, however (see e.g., *ENISA (2017b))*, but this might be due to developments in the security assessments in the last few years.

[121] *Datatilsynet (2017)*; *ICO (2019b)*, p. 15-16.

[122] *ICO (2019b)*, p. 16; *NCSC (2017)*.

[123] *Digitaliseringsdirektoratet [The Norwegian Digitalisation Agency] (2020)* has presented some recommendations on this, but they seem to be the only government body to have done so specifically so far (as far as my research has shown).

[124] *NSM (2016)*.

[125] *ICO (2019b)*, p. 15, referring to *NIST (2014)*.

[126] *CFCS (2020)*.

[127] *NCSC (2017)*.

4.4.2 E-mail

Perhaps the most vital information flow in any organisation today, is e-mail communication. Unless there is very sensitive information being transferred, and strict procedures in place for protecting it, most organisations will consider e-mails being sent internally as information within the organisation. This is reasonable, but only if the necessary measures are taken to ensure the confidentiality of the e-mails.[128]

TLS is also the standard which is recommended to keep e-mails secure in transit, and both the Norwegian Digitalisation Agency and the NCSC supply recommendation on its use and implementation.[129] There are, however, additional measures that can be taken to ensure end-to-end encryption of the e-mail, which goes one step further than TLS. Some of these methods are PGP and S/MIME, and rely on key generation between the communicating parties, and for S/MIME also a certificate authority. The Danish DPA has published a guide on the most common methods.[130] In addition, both the Norwegian and French DPAs refer to the open-source version OpenPGP (GNU Privacy Guard) to ensure secure communication.[131]

Finally, one of the most secure methods to transmit sensitive data by e-mail, albeit inconvenient, are password-protected attachments. If the password is strong, and a recommended version of symmetric encryption is used (see chapter 3.3), this might be a good alternative. This method requires that both parties have the encryption key, or that this is being transmitted through another, secure channel.[132]

4.4.3 Other types of communication

The benefit with the above-mentioned methods is that they are well-known, easy to identify to the user, and readily available. For all services not running over any of the protocols mentioned above, we will need to assess the application and its security measures, as far as this is possible to do. Most applications on a computer or apps on a mobile device communicate with its servers, or even other users. If the communication is business-critical, or particularly if it may contain personal data, we are required to take reasonable precautions in ensuring the systems and applications we use keep the data secure.[133]

---

[128] While outside the scope of this thesis, we should note that fake e-mails produced to gain access to a system ('phishing') are one of the largest IT security issues today – and necessary measures to stop such attempts, or limit their damage potential is extremely important to all businesses with an online presence.

[129] *Digitaliseringsdirektoratet [The Norwegian Digitalisation Agency] (2020)*; *NCSC (2019).*

[130] *Datatilsynet (DK) [The Danish DPA] (2020)*.

[131] *Datatilsynet [The Norwegian DPA] (2018b)*, *CNIL (2018).*

[132] *Datatilsynet (DK) [The Danish DPA] (2020).*

[133] *ICO (2019b)*, p. 14; *NCSC (2018)*.

The sources mentioned are very reserved in recommending specific applications, and it is therefore up to the organisations themselves to assess whether the systems they use provide the appropriate security, also when it comes to encrypting data. If no recommendations or standards are available, it is necessary to consult technical documentation, independent reviews or audits, or any other relevant source on the application. A good example of the challenges in this, was the video conference application Zoom which had promised its users end-to-end encryption, whereas security researchers discovered that the company had the encryption key to any conference call made – which under no circumstance should be advertised as end-to-end encryption.[134]

4.5 Guidance on cloud services

Cloud services implies outsourcing digital services which would otherwise be accomplished through the organisation's own devices and on networks and systems controlled by the organisation. Cloud services have grown to be immensely popular, particularly among small- and medium-sized organisations, largely due to the efficiency of sharing offsite networks for optimal performance, and due to most security aspects now being dealt with by a professional service provider.[135]

However, cloud services are not the one-size-fits-all-measure many business leaders take them to be. They comprise a range of different services with different service providers, on different systems with many different security approaches. As such, using cloud services does not absolve anyone from their responsibilities under the relevant regulation if they do not make the necessary *research* into what the cloud services can and cannot do.

For encryption purposes, cloud services require the same type of considerations as when an organisation's own devices are used. The only difference is that the systems and devices themselves are offsite, meaning you need to rely on the cloud service provider to ensure that the data you store on their systems are securely encrypted, and that all data transferred between your organisation's devices and the cloud-based systems are securely transferred. This is an important point to keep in mind: Effectively, this means that all the data which used to be processed on your own devices, are now being constantly transferred over the internet with the same possibility of attack as all other data on the internet is subject to.

---

[134] *McCarthy (2020)*. See above on symmetric encryption in chapter 3.3.

[135] Furthermore, the cloud service provider would be considered a DSP under the NIS Directive, and subject to the corresponding regulation (as discussed in chapter 2.2). Note that this would not limit the responsibility for data security for the organisation procuring the cloud service, but it could impact the final assessment of appropriateness.

The sources I have reviewed can give no definitive answers on what a secure cloud service looks like, let alone how data will need to be encrypted. NCSC has presented a comprehensive guidance on what considerations to make in its 'Cloud security guidance', where they present 14 'cloud security principles'.[136] Among these, two deserve particular mention:

- *Data in transit protection*
- *Asset protection and resilience*

Under *Data in transit protection*, the NCSC introduces five methods and a general assessment:

- Private WAN service: Hard to intercept, but need additional encryption enabled to be sufficiently secure.
- Legacy SSL and TLS: Not secure and not recommended.
- TLS (Version 1.2 or above): Has security issues, but these may be managed through using recent, supported and fully patched versions of TLS.
- IPsec or TLS VPN gateway: Can be secure if correctly set up (see NCSC's own guide on secure configurations of IPSec[137]).
- Bonded fibre optic connections: Secure if independently audited and with sufficient monitoring.

Under *Asset protection and resilience*, the recommendation to have all physical storage on the cloud service encrypted[138] seems clear enough but does not give any further information. We might reasonably infer from a recommendation to ensure encryption levels at least as high as would have been implemented on their own systems.

One last element in the NCSC guidance is principle 13: *Audit information for users*. Technically, this is beyond the scope of this thesis, but independent auditing of the service is in reality the only way to know if you are getting the security and the encryption you are required to have to comply with the relevant regulation (and also, which you are paying for). The recommendation of the NCSC implies that a lack of sufficient audit information gives reason to doubt the security level being appropriate, even if the cloud service has promised such.

NSM has also produced guidance on the use of cloud services. In general, the importance of risk assessment and the understanding of the cloud service's security capabilities are some of

[136] *NCSC (2018b)*.

[137] *NCSC (2016)*. See also *NSM (2020b)*, p. 32.

[138] See *NCSC (2018)*, Implementing the Cloud Security Principles - 2.3 Data at rest protection.

the core elements in this guidance.[139] Also, the NSM stresses the need for independent assessments of the encryption methods and capabilities, and, most importantly, they point out how easily a cloud service provider can access encrypted data due to the data in fact being accessed on their systems (see chapter 2.3 on *data in use* above, and the difficulties in accessing data without encrypting it).[140] This threat factor may possibly be mitigated, or at least better managed, through FHE[141].

Finally, one must always remember that the use of cloud services cannot be made possible without any types of devices owned and controlled by the organisation. Even if all documents are stored and edited on cloud services, the user must nevertheless access the cloud service to issue the necessary commands from a computer, a tablet, or any other terminal equipment. This equipment is now even more vulnerable, because it allows an unauthorised user to access the cloud services if the device is hacked or stolen, and there are no security mechanisms in place. For this reason, the use of cloud services leaves no reason to relax the security levels for onsite equipment – on the contrary, most of the guidance above is still highly relevant.

4.6 Next-level guidance on encryption

There are bound to be more or less available sources that should have had their recommendations presented and discussed above (keep in mind that every EU country has a DPA, and most also have a cybersecurity agency, all with their own recommendations), but the scope of this thesis only allows a relevant selection of sources. At a certain level of abstraction such sources have their limitations, and one is gradually referred to the technical literature.

We also find several references to sector-based guidance, where these are in place. This will in many cases be the recommendations of special interest groups, such as the European Payments Council (EPC) and their guidelines within the banking sector on the use of encryption.[142] These are important recommendations, particularly considering this sector being under constant scrutiny by their respective DPAs.[143] Another sector with particular guidance available is video surveillance.[144]

---

[139] *NSM (2020d)*.

[140] *NSM (2020e)*.

[141] Fully homomorphic encryption, see chapter 3.3.

[142] *EPC (2020)*. See pp. 9-13 for recommendations and best practices.

[143] See for instance the MisterTango UAB data breach case brought by the Lithuanian DPA, and the case brought by the Italian DPA (Garante) against the Italian Revenue Agency for unencrypted e-invoices, cf. *EDPB (2019b) and (2019c)*.

[144] *EDPB (2019d)*, ch. 5.2.

In some cases, an organisation needs to go further to ensure an appropriate security level. This can be particularly important when the data processed is critical to the assignment an organisation is set out to achieve, to a level where there is a pressing need to *document* compliance at a higher level. Technical literature is hard to assess, and continuous consultancy can be inconsistent and costly. In such cases, *standardisation* is a security expert's best friend.

I have earlier mentioned *ISO/IEC 27001:2013 (2019)*, which is a general standard dealing with information security. It is an important starting point in the security assessment of an organisation, which is why it is frequently referenced by other sources.[145] There are, however, other standards which should be considered for specific needs. *FIPS 140-3 (2019)* is often referenced by cybersecurity agencies and DPAs, and can rightfully be considered an authoritative source for the state of the art at the time of publication.[146] FIPS 140-3 does not include any recommendations itself, but is instead aligned with *ISO/IEC 19790:2012 (2018)*.

This standard bears the title *Security requirements for cryptographic modules* and is possibly one of the most comprehensive and detailed descriptions on how the state of the art of cryptography looks. Unfortunately, it is only available through the national ISO-office at a very stiff price, and this appears to be the only way to get a hold off it.[147] Its contents *may* be of importance to some organisations, particularly due to it being one of very few sources outlining encryption requirements on different security levels, according to the information given by ISO:

> 'This International Standard defines four security levels for cryptographic modules to provide for a wide spectrum of data sensitivity (e.g. low value administrative data, million dollar funds transfers, life protecting data, personal identity information, and sensitive information used by government) and a diversity of application environments (e.g. a guarded facility, an office, removable media, and a completely unprotected location). This International Standard specifies four security levels for each of 11 requirement areas with each security level increasing security over the preceding level.'[148]

For anyone seeking to fully understand what encryption should be used at a given *appropriate security level having regard to the state of the art*, this standard – with its levelled descriptions – seems to be the right way to go. The fact that it is referenced by many authoritative sources (primarily via FIPS 140-3 mirroring its content), gives further weight to this argument.

---

[145] See footnote 76 for examples of references to this standard.

[146] See e.g., *ICO (2019b)*, p. 23.

[147] No academic institution in Norway has access to the standard itself, and it also appears to be rarely cited and discussed in academic literature. My information on the standard is therefore limited to the information given by ISO on its web page.

[148] *ISO/IEC 19790:2012 (2018)*, 'Abstract'.

On the other hand, there is the question of availability – does this standard go beyond what organisations can reasonably be required to have knowledge of? Most organisations must be expected to do a certain amount of research on their encryption needs, but it seems fair that this should be limited to open and available sources, and that only organisations with particularly sensitive data processing can be expected to delve this deep into the subject matter. Having said that, compared to an ordinary IT budget for a business relying on digital services in 2020, 178 Swiss francs can hardly be considered an excessive investment – not least if it goes a long way in guaranteeing compliance.[149]

For those organisations having such special needs in encryption, there are also other sources which may be of interest. The *NIST Cryptographic Algorithm Validation Program (CAVP)* gives up-to-date info on algorithm validation, effectively giving updated insight into the technical capabilities.[150] Beyond the recommendations from ENISA mentioned above, there are also a number of detailed recommendations and reports, which in spite of their age (more than five years old) may supply more detailed information of interest.[151]

Finally, the subject of *steganography* deserves mention.[152] This is the concept of not simply encrypting data, but also to conceal the transmission of the data in question. This is usually done through injecting data into packages containing other types of data, giving the appearance that this package for example contains HTTPS-data from a web site, when the fact is that someone is communicating by a voice call. This method is usually combined with encryption schemes, but it needs to be subtle – the opponent is here someone who is looking for a specific type of communication. While not encryption per se, it is a communication method which may be needed, if an employee of an organisation should need to communicate offsite from a high-risk area, where most data communication not specifically allowed, is blocked.[153]

5 Harmonisation and future-proofing encryption requirements

5.1 An appropriate security level and the state of the art

Having reviewed the relevant sources above, it is possible to draw some conclusions as to what an *appropriate security level* might be in terms of cryptographic techniques, and also what the

[149] *ISO/IEC 19790:2012 (2018)*

[150] *NIST (2020)*.

[151] See *ENISA (2012)*, *(2013)*, *(2014a)* and *(2014b)*.

[152] *NOU 2015: 13*, pp. 50-51.

[153] For example the 'Great Firewall of China', which controls all internet traffic going in and out of the PRC. See *Wang (2020*) for a short historical introduction.

state of the art in encryption methods can be regarded, at least at the time of any particular recommendation's preparation. More importantly, however, they give us insight into the *method* which should be used to comply with the security level required by the relevant regulation. If an organisation is to adhere by the requirements set out in the regulation, and establish the measures needed to do this, there must be a reasonable method for it to understand what level they should be at, and what measures are sufficient to be at this level – at any given time.

None of the sources I have discussed, gives a clear answer to any organisation. As is often the case when law is to be interpreted, the answer is among the lines of 'it depends'. And it usually depends on the type of data being processed, and how bad it would be if it were accessed by an unauthorised entity. The more sensitive the data, the stronger encryption is to be expected by the organisation. The need for a high level of security also affects the knowledge question: the more sensitive the data being processed is, the more research into what constitutes strong encryption is required of the organisation. In short, if you understand your data to be particularly sensitive, you are also expected to spend more time and resources to find what encryption methods are needed to ensure an appropriate security level.

The sources are fairly specific on what type of cryptographic techniques should be used, considering the state of the art. This is useful when designing a system to process your data, because you know exactly what encryption level you *at least* need to implement. But it is not very practical when you are to decide on a specific system or application/software, unless they supply this information at a level of abstraction enabling the customer to assess these facts. Comparing the detailed recommendations reviewed above with the technical information usually supplied by consumer-grade data processing systems leaves much to be desired.[154]

5.2 Standardisation

At the same time, this seemingly impossible task of establishing an appropriate level of security is also somehow true to the regulation from which it springs. The relevant regulation is clearly intended to be *technology-neutral*, meaning a definite answer to the question of a certain security level for a certain type of data will only be temporary. An organisation is always expected to seek information on what security measures are appropriate for its activity in general, and how data is to be encrypted in particular.[155] In addition, this level also needs to be future-

[154] During my research, I made some attempts at comparing the encryption used by popular cloud services, as an example. All services stress that they use both at rest- and in transit-encryption, but few give details on what methods are used. The most one is likely to find is a reference to AES-256, but nothing on mode of operation or further details. There seems also to be a great deal of misinformation and unconfirmed information on encryption used by competitors, further complicating such research.

[155] See chapter 4.1 for the discussion on whether encryption will always be required under the relevant regulation. As there are hardly any cases where encryption should not be implemented, I focus on the 'how' rather than the 'if'.

proofed, meaning it should not only be secure against the threats of today, but also those which can reasonably be expected tomorrow.

Standards are an excellent way to simplify this assessment, and the relevant regulation already seems to point towards any standards which would be helpful. They need to be based on recent technical insight, and be updated and confirmed – so that the public knows the information may be considered a reflection of the state of the art. Still though, complying with a standard does not replace the necessary research required to understand the technical requirements.

Throughout chapter 4, I have discussed a number of standards: some are too vague on the subject of encryption (e.g., ISO/IEC 27001:2013), some are difficult to access (e.g., ISO/IEC 19790:2012), whereas others are sector-specific – which is very useful if you operate within that sector, but not if this is not the case. Perhaps most interesting are the certification schemes expected to arrive with the Cybersecurity Act, which by and large seems to be the EU's approach at making it easier to assess an appropriate security level. This is, after all, not an uncommon development in European law: first a rough measure given through the proportionality principle, and then subsequent regulation providing more details as to what is required to comply.

At the time of writing, there exists no EU-based certification scheme for encryption.[156] There will likely be a number of relevant certifications introduced eventually, but it is unknown what this will mean for the encryption levels required under the current relevant regulation. Still, the larger framework of cybersecurity under EU law seems to suggest that a technology-neutral, future-proof encryption compliance scheme, would reasonably require detailed EU-based standards, preferably with the option to be certified towards the levels required.

5.3 Conclusions

Until this is in place, we are left with the technical insight, recommendations, guidance, and best practices which we find in the sources discussed in chapter 4. The sources included are only a handful of all those agencies and other authoritative sources available, but I believe they represent a solid outline of how organisations should and could protect the data they process. The organisation itself must assess and decide what level of protection the data they process needs (e.g., personal data, business-critical data, customer correspondence, etc.). Even though the wording in the GDPR and the NIS Directive are similar, the assessment needs to consider the different needs of protection corresponding to the type of data being processed.

[156] The European Cybersecurity Certification Group (ECCG) does not seem to report on any certifications as far as can be read from the information on their website, see *European Commission (2020)*.

Through the sources, we see relatively detailed recommendations available for the more security-critical types of data. Beyond this, we are also given a fair overview of the recommendations of lower-level security encryption, albeit at a higher level of abstraction, and sometimes with minor differences. Details are important here, as we are dealing with mathematical functions and algorithms – technically speaking, an exact science, not least compared to the margins of appreciation usually afforded in the legal sciences.

What makes these sources valuable, is the fact that they usually will be sufficient for employees with technical insight to, in most cases, advise their superiors on the ideal choice of protection. It allows an organisation to work with the material available and behave accordingly. The relevance of this is important: when an organisation can show to relevant, competent personnel being tasked with assessing security levels and recommendations to encryption schemes, and this is documented (e.g., through internal memos), it stands to reason that an organisation heeding the advice given, and putting the necessary measures in place, *will be in compliance with the relevant regulation*.

Such a method might seem overly careful, but if there is one element to take from this thesis, it is this: Deciding what is an appropriate security level, having regard to the state of the art, is a task which can only be completed at a *reasonable level*, meaning that any organisation must demonstrate its best effort to *understand* compliance, and in turn, to do what is necessary to *be* in compliance.

Finally, one more point must be stressed, and can perhaps never be stressed enough. Encryption, while a very important security measure, is still only one of many available security measures which may ensure an appropriate security level under the relevant regulation. A computer system is only as secure as its weakest link, and even the best encryption available cannot mitigate insufficient security for another element in the system. Most security breaches having surfaced happen not because of lacking encryption (even though this also happens, as we have seen), but *in spite* of good encryption being in place. To borrow an oft-cited analogy: Even the most secure door will fail in keeping intruders out, if the window is open.[157]

6 Final remarks

There should be no doubt about it: Interpreting the relevant regulation and applying it when an organisation is deciding on a method to process the data it deals with in its operations, is challenging. And establishing a common framework on how this is to be done, is a borderline hopeless task. I believe, however, that through this jungle of recommendations, guidance, standards,

[157] *Harris and Maymi (2018)*, ch. 1.

technical literature – and even statutory law – I have been able to identify a number of *core elements* relevant to the choice of encryption method to use with the data. By doing as much research as possible with the information given, and always asking the right questions in procurement or development processes, one would in most cases be able to steer the organisation into compliance with a fair margin.

It is obviously a methodological challenge to review two sets of regulation, dealing with seemingly different types of data processing. The GDPR has had a few years to mature, and its concepts of security measures and data protection by design are today well implemented in the Union (but not always with all organisations, as the fines imposed in later years from DPAs bear witness of). The NIS Directive, however, has only recently been implemented in EU countries, and are in the process of being implemented in the EEA countries. Considering the wording and the risk situation for cybersecurity in general, I find it reasonable to expect that the two sets of regulation will be largely interconnected in the years to come – meaning that advice and recommendations will be mutually relevant. This also seems to be in the intention for both sets of regulation, and at a higher level, not an uncommon way to deal with the establishment of new regulation under EU law.[158] There is of course no guarantee for these regulations to develop in this manner, but at the time of writing this appears to me to be the most likely way forward.[159]

This thesis has only scratched the surface of encryption as a security measure, and how the EU is attempting to ensure its widespread usage. Ironically, most academic interest in the subject seems to centre on the issue of governments wanting to control and limit the use of encryption, for their own policing and intelligence needs, whereas EU law focuses on the organisations putting in place sufficient security measures to protect both the data being processed (which is valuable to both citizens and the organisations), and to ensure the well-functioning of the markets, and the stability of the nation states and the union as a whole. While much could be said and written about the difference in approaches on encryption – both in the world today, and historically – this is beyond the scope of this thesis. And the same goes for the coming development of the relevant regulation discussed here: this will be up to other researchers to delve into.

[158] See *Michels and Walden (2020)* for a discussion on the interplay between governments and the EU on the NIS Directive so far.

[159] See chapter 2.2 for more on the methodological decisions taken.

7 Table of reference[160]

7.1 Norwegian legal sources

7.1.1 Statutory law

EØS-loven [The EEA Act]	Lov om gjennomføring i norsk rett av hoveddelen i avtale om Det europeiske økonomiske samarbeidsområde (EØS) m.v. (EØS-loven) [Act implementing the main part of the Agreement on the European Economic Area etc. into Norwegian law – The EEA Act] (1992-11-27-109).
Helseregisterloven [The Personal Health Data Filing System Act]	Lov om helseregistre og behandling av helseopplysninger (helseregisterloven) [Personal Health Data Filing System Act] (2014-06-20-43).
Personopplysningsloven [The Personal Data Act]	Lov om behandling av personopplysninger (personopplysningsloven) [The Personal Data Act] (2018-06-15-38).
Sikkerhetsloven [Act on National Security / The Security Act]	Lov om nasjonal sikkerhet (sikkerhetsloven) [Act on National Security / The Security Act] (1998-03-20-10).

7.1.2 Preparatory works

Høringsnotat om utkast til lov som gjennomfører NIS-direktivet i norsk rett (2018)	Justis- og beredskapsdepartementet [The Norwegian Ministry of Justice and Public Security] (2018), *Høringsnotat om utkast til lov som gjennomfører NIS-direktivet i norsk rett [Consultative paper on the draft bill implementing the NIS Directive in Norwegian law]*, 21. December 2018.

[160] The left column is the citation used in the text or in footnotes, while the full citation is in the right column.

Meld. St. 5 (2020-2021) — Justis- og beredskapsdepartementet [The Norwegian Ministry of Justice and Public Security], *Meld. St. 5 (2020-2021). Samfunnssikkerhet i en usikker verden [Report to the Storting – White Paper]*, 16. October 2020.

Norsk kryptopolitikk (2019) — Forsvarsdepartementet [The Norwegian Ministry of Defence] and Justis- og beredskapsdepartementet [The Norwegian Ministry of Justice and Public Security] (2019), *Norsk kryptopolitikk [Norwegian Encryption Policy]*, Policy Paper.

NOU 2015: 13 — NOU 2015: 13: *Digital sårbarhet – sikkert samfunn* (Lysne-utvalget) [The Lysne Commission – Official Norwegian Report].

NOU 2018: 14 — NOU 2018: 14: 'IKT-sikkerhet i alle ledd' (Holte-utvalget) [The Holte Commission - Official Norwegian Report].

7.1.3 Official guidance and recommendations

Datatilsynet (2017) — Datatilsynet [The Norwegian DPA] (2017), 'Kryptering' [Encryption], last updated 7. March 2017 (retrieved from https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/informasjonssikkerhet-internkontroll/kryptering/ on 2020-10-23).

Datatilsynet (2018a) — Datatilsynet [The Norwegian DPA] (2018), 'Etablere internkontroll - Iverksette styringssystem for informasjonssikkerhet' [On the establishment of control systems for information security], last updated 30. October 2018 (retrieved from https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/informasjonssikkerhet-internkontroll/etablere-internkontroll/iverksette-styringssystem-for-informasjonssikkerhet/ on 2020-11-05).

Datatilsynet (2018b) — Datatilsynet [The Norwegian DPA] (2018), *Veiledning i kryptering med OpenPGP* [Guidance on encryption with OpenPGP], last updated 18. September 2018 (retrieved from https://www.datatilsynet.no/om-datatilsynet/kryptering-med-openpgp/ on 2020-11-10).

Datatilsynet (2019a) Datatilsynet [The Norwegian DPA] (2019), 'Sikkerhetsarkitektur' [Security Architecture], last updated 16. July 2019 (retrieved from https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/informasjonssikkerhet-internkontroll/sikkerhetsarkitektur/ on 2020-11-05).

Datatilsynet (2019b) Datatilsynet [The Norwegian DPA] (2019), 'Programvareutvikling med innebygd personvern - Koding' [On software development and programming towards the goal of privacy by design], last updated 20. August 2019 (retrieved from https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/innebygd-personvern/programvareutvikling-med-innebygd-personvern/koding/ on 2020-11-07).

Datatilsynet (2020) Datatilsynet [The Norwegian DPA] (2020), 'Retningslinjer for bruk av videoenheter - Behandling av særlige kategorier personopplysninger' [Guidance on the use of video equipment – Processing of special categories of personal data], last updated 14. September 2020 (retrieved from https://www.datatilsynet.no/regelverk-og-verktoy/internasjonalt/retningslinjer-og-uttalelser-fra-personvernradet/retningslinjer-for-bruk-av-videoenheter/behandling-av-sarlige-kategorier-personopplysninger/ on 2020-10-29)

Digitaliseringsdirektoratet (2020) Digitaliseringsdirektoratet [The Norwegian Digitalisation Agency] (2020), *Grunnleggende datakommunikasjon* – Referansekatalogen for IT-standarder *[Basic computer communications – The reference catalogue on IT standards]* (retrieved from https://www.digdir.no/digitale-felleslosninger/grunnleggende-datakommunikasjon/1488 on 2020-11-10).

NSM (2015) Norsk Sikkerhetsmyndighet (NSM) [Norwegian National Security Authority] (2015), *Sikkerhetsfaglig råd 2015 [Technical Advice on Security Topics]*, (retrieved from https://www.regjeringen.no/globalassets/departementene/fd/dokumenter/rapporter-og-regelverk/nsm-sikkerhetsfaglig_raad_2015_web.pdf on 2020-10-23).

NSM (2016) Nasjonal Sikkerhetsmyndighet (NSM) [Norwegian National Security Authority] (2016), *Sikring av kommunikasjon med TLS - Beskrivelse av grunnleggende tiltak for sikring kommunikasjon over usikre nett ved hjelp av TLS*, last updated 30. September 2016 (retrieved from https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/sikring-av-kommunikasjon-med-tls/ on 2020-11-10).

NSM (2020a) Nasjonal Sikkerhetsmyndighet (NSM) [Norwegian National Security Authority] (2020), *Håndbok i beskyttelse av skjermingsverdig ugradert informasjonssystem [Handbook on the protection of information systems processing unclassified sensitive data]*, v. 1.04, 22. April 2020 (retrieved from https://nsm.no/regelverk-og-hjelp/veiledere-og-handboker-til-sikkerhetsloven/handbok-i-beskyttelse-av-skjermingsverdig-ugradert-informasjons-system/om-denne-handboken/ on 2020-10-17).

NSM (2020b) Nasjonal Sikkerhetsmyndighet (NSM) [Norwegian National Security Authority] (2020), *Grunnprinsipper for IKT-sikkerhet [Fundamental principles for security in information and communication technology]*, v. 2.0, April 2020 (retrieved from https://nsm.no/fagomrader/digital-sikkerhet/rad-og-anbefalinger-innenfor-digital-sikkerhet/grunnprinsipper-ikt on 2020-11-05).

NSM (2020c) Nasjonal Sikkerhetsmyndighet (NSM) [Norwegian National Security Authority] (2020), *NSM Cryptographic Recommendations*, v. 1.0, last updated 12. June 2020[161] (retrieved from https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/nsm-cryptographic-recommendations/ on 2020-11-07).

NSM (2020d) Nasjonal Sikkerhetsmyndighet (NSM) [Norwegian National Security Authority] (2017), *Sikkerhetsfaglige anbefalinger ved tjenesteutsetting [Technical recommendations on outsourcing]*, last updated 27. July 2020 (retrieved from https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/sikkerhetsfaglige-anbefalinger-ved-tjenesteutsetting/introduksjon/ on 2020-11-11).

[161] The document itself is undated, and the date on NSM's web site seems to be corresponding with the launch of its new web site. A previous (now dead) link (https://www.nsm.stat.no/globalassets/dokumenter/veiledninger/systemteknisk-sikkerhet/nsmcryptographic-recommendations-juli19.pdf) seems to suggest the document in its current version was published in July 2019.

NSM (2020e) Nasjonal Sikkerhetsmyndighet (NSM) [Norwegian National Security Authority] (2017), *Sky, tjenesteutsetting og sikkerhet - Spørsmål om sky og tjenesteutsetting [Cloud, outsourcing and security - Q&A]*, last updated 28. August 2020 (retrieved from https://nsm.no/fagomrader/digital-sikkerhet/rad-og-anbefalinger-innenfor-digital-sikkerhet/sky-tjenesteutsetting-og-sikkerhet on 2020-11-11).

7.2 International legal sources

7.2.1 International law

The EEA Agreement Agreement on the European Economic Area (The EEA Agreement), original agreement signed 2 May 1992.

7.2.2 EU directives and regulation

Directive 95/46/EC (Data Protection Directive – DPD) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive – DPD).

Directive 2002/58/EC (The e-Privacy Directive) Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

Directive (EU) 2016/1148 (The Network and Information Systems Directive – The NIS Directive) 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 (The General Data Protection Regulation – GDPR)	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.
Commission Implementing Regulation (EU) 2018/151 (NIS implementation 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.
Regulation (EU) 2019/881 (Cybersecurity Act)	Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013.

7.2.3 EU-based guidance and recommendations (also DPAs outside of Norway)

CNIL (2018)	Commission Nationale Informatique & Libertés (CNIL) (2018), *Security of Personal Data*, The CNIL's Guides (retrieved from https://www.cnil.fr/en/new-guide-regarding-security-personal-data on 2020-11-30).
Datatilsynet (DK) [The Danish DPA] (2018)	Datatilsynet [The Danish DPA] (2018), Behandlingssikkerhed. Databeskyttelse gennem design og standardindstillinger [Security in data processing. Data protection by design and default], last updated June 2018 (retrieved from https://www.datatilsynet.dk/media/7587/artikel25og32-vejledning.pdf on 2020-11-25).
Datatilsynet (DK) [The Danish DPA] (2020)	Datatilsynet [The Danish DPA] (2020), *Transmission af personoplysninger via e-mail* [Transmission of personal data by e-mail], last updated on the time of retrieval (undated) (retrieved from https://www.datatilsynet.dk/emner/persondatasikkerhed/transmission-af-personoplysninger-via-e-mail on 2020-11-10).

ENISA (2012) European Union Agency for Cybersecurity (ENISA) (2012), *Study on the use of cryptographic techniques in Europe*, December 2011, updated April 2012 (retrieved from https://www.enisa.europa.eu/publications/the-use-of-cryptographic-techniques-in-europe on 2020-11-14).

ENISA (2013) European Union Agency for Cybersecurity (ENISA) (2013), *Securing personal data. Recommended cryptographic measures*, 20. September 2013 (retrieved from https://www.enisa.europa.eu/publications/recommended-cryptographic-measures-securing-personal-data on 2020-11-14).

ENISA (2014a) European Union Agency for Cybersecurity (ENISA) (2014), *Study on cryptographic protocols*, December 2017 (retrieved from https://www.enisa.europa.eu/publications/study-on-cryptographic-protocols on 2020-11-14).

ENISA (2014b) European Union Agency for Cybersecurity (ENISA) (2017), *Algorithms, key size and parameters report*, November 2014 (retrieved from https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014 on 2020-11-14).

ENISA (2017a) European Union Agency for Cybersecurity (ENISA) (2017), *Guidelines for SMEs on the security of personal data processing*, December 2017 (retrieved from https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing on 2020-10-28).

ENISA (2017b) European Union Agency for Cybersecurity (ENISA) (2017), *Handbook on Security of Personal Data Processing*, December 2017 (retrieved from https://www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing on 2020-11-09).

EDPB (2019a) European Data Protection Board (EDPB), *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*, 13. November 2019 (retrieved from https://edpb.europa.eu/our-work-

tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en on 2020-10-15).

EDPB (2019d) European Data Protection Board (EDPB), *Guidelines 3/2019 on processing of personal data through video devices*, 13. November 2019 (retrieved from https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en on 2020-10-15).

ICO (2019a) Information Commissioner's Office (ICO) (2019), *Guide to the General Data Protection Regulation (GDPR)*, v 1.0.729, 22. May 2019 (retrieved from https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/ on 2020-10-28).

ICO (2019b) Information Commissioner's Office (ICO) (2019), *The General Data Protection Regulation - Encryption*, v 1.0.7, 24. April 2019 (retrieved from https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/ on 2020-10-28).

7.2.4 Other guidance and recommendations

CFCS (2020b) Center for cybersikkerhed [Centre for Cybersecurity] (CFCS) (2020), *Retningslinjer for sikker brug af Transport Layer Security (TLS)* [Guidance on secure use of TLS], Vejledning [Guidance], 1. ed., October 2020 (retrieved from https://cfcs.dk/da/forebyggelse/vejledninger/tls/ on 2020-11-10).

EPC (2020) European Payments Council (EPC) (2020), *Guidelines on cryptographic algorithms usage and key management*, EPC342-08 Version 9.0, 9. March 2020 (retrieved from https://www.europeanpaymentscouncil.eu/document-library/guidance-documents/guidelines-cryptographic-algorithms-usage-and-key-management on 2020-11-11).

NCSC (2016) National Cybersecurity Centre (NCSC), *Using IPsec to protect data*, last updated 23. September 2016 (retrieved from https://www.ncsc.gov.uk/guidance/using-ipsec-protect-data on 2020-11-10).

NCSC (2017) National Cybersecurity Centre (NCSC), *Using TLS to protect data*, last updated 17. December 2017 (retrieved from https://www.ncsc.gov.uk/guidance/tls-external-facing-services on 2020-11-10).

NCSC (2018a) National Cybersecurity Centre (NCSC), *GDPR Security Outcomes*, v. 1.0, 17. May 2018 (retrieved from https://www.ncsc.gov.uk/guidance/gdpr-security-outcomes on 2020-10-23).

NCSC (2018b) National Cybersecurity Centre (NCSC), *Cloud security guidance*, v. 1.0, 17. November 2018 (retrieved from https://www.ncsc.gov.uk/collection/cloud-security on 2020-11-11).

NCSC (2019a) National Cybersecurity Centre (NCSC), *Email security and anti-spoofing*, v. 2.0, 7. October 2019 (retrieved from https://www.ncsc.gov.uk/collection/email-security-and-anti-spoofing on 2020-11-10).

NCSC (2019b) National Cybersecurity Centre (NCSC), *NCSC CAF guidance - B.3 Data security*, v. 3.0, 30. September 2019 (retrieved from https://www.ncsc.gov.uk/collection/caf/caf-principles-and-guidance/b-3-data-security on 2020-11-25).

NIST (2014) National Institute of Standards and Technology (NIST) (2014), *Guidance for the Selection, Configuration and Use of Transport Layer Security (TLS) Implementations*, Special Publication 800-52 Revision 1 (retrieved from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r1.pdf on 2020-11-10).

NIST (2020) National Institute of Standards and Technology (NIST) (2020), *Cryptographic Algorithm Validation Program (CAVP)* (retrieved

from https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program on 2020-11-12).

7.2.5 Standards

FIPS 140-3 (2019) — Federal Information Processing Standards (FIPS) (2001) (2019), *Publication 140-3: Security Requirements for Cryptographic Modules* (FIPS PUB 140-3) (retrieved from https://csrc.nist.gov/publications/detail/fips/140/3/final on 2020-11-30).

FIPS 197 (2001) — Federal Information Processing Standards (FIPS) (2001), *Publication 197: Advanced Encryption Standard (AES)* (FIPS PUB 197) (retrieved from https://csrc.nist.gov/publications/detail/fips/197/final on 2020-11-30).

ISO/IEC 15408 — ISO/IEC 15408-1:2009, *Information technology — Security techniques — Evaluation criteria for IT security*, last reviewed and confirmed in 2015 (retrieved from https://www.iso.org/standard/50341.html on 2020-11-15).

ISO/IEC 27001:2013 — ISO/IEC 27001:2013, *Information technology — Security techniques — Information security management systems — Requirements*, last reviewed and confirmed in 2019 (retrieved from https://www.iso.org/standard/54534.html on 2020-11-12).

ISO/IEC 19790:2012 (2018) — ISO/IEC 19790:2012, *Information technology — Security techniques — Security requirements for cryptographic modules*, last reviewed and confirmed in 2018 (retrieved from https://www.iso.org/standard/52906.html on 2020-11-12).

RSA Laboratories (1999) — RSA Laboratories (1999), *PKCS #1 v2.1: RSA Cryptography Standard*, republished as RFC (Request for Comments) 3447 (and later, in v.2.2, as RFC 8017) (retrieved from https://tools.ietf.org/html/rfc3447 and https://tools.ietf.org/html/rfc8017 on 2020-11-30).

7.3 Literature and other sources

Aumasson (2018) — Aumasson, Jean-Philippe (2018), *Serious cryptography. A practical introduction to modern encryption*, San Francisco: No Starch Press.[162]

Baratta (2014) — Baratta, Roberto (2014), 'Complexity of EU Law in the Domestic Implementing Process', *The Theory and Practice of Legislation* 2 (3), pp. 293-308.

CFCS (2020a) — Center for cybersikkerhed [The Centre for Cyber Security (DK)] (CFCS) (2020), *Ordforklaringer [Definitions]* (retrieved from https://cfcs.dk/da/cybertruslen/ordforklaringer/ on 2020-11-03).

Chopra and Chaudhary (2020) — Chopra, Abhishek and Mukund Chaudhary (2020), *Implementing an Information Security Management System: Security Management Based on ISO 27001 Guidelines*, Berkeley: Apress.

CPDP (2020) — Computer, Privacy and Data Protection (CPDP) Conference 2020, Brussels, Belgium, 'The State of the Art Requirement for GDPR Security Measures', 22. January 2020.

Darknet Diaries (2018) — Darknet Diaries (2018), 'Crypto Wars', Season 1 Episode 12, 1. February 2018 (retrieved from https://darknetdiaries.com/episode/12/ on 2020-10-17).

EDPB (2019a) — European Data Protection Board (EDPB) (2019), *First Significant Fine Was Imposed for the Breaches of the General Data Protection Regulation in Lithuania*, Press Release, 21. May 2019 (retrieved from https://edpb.europa.eu/news/national-news/2019/first-significant-fine-was-imposed-breaches-general-data-protection_en on 2020-11-11).

[162] The online version of the book unfortunately does not include page numbers, and I have therefore had to limit citations to chapter number. Due to the libraries being closed at the time of writing (covid-19 restrictions), I have also been unable to consult the printed version.

EDPB (2019b) European Data Protection Board (EDPB) (2019), *Italian Garante - E-invoices: No Database to be set up by Italy's Revenue Agency. No E-invoices for Health Care Services*, Press Release, 20. March 2019 (retrieved from https://edpb.europa.eu/news/national-news/2019/italian-garante-e-invoices-no-database-be-set-italys-revenue-agency-no-e_en on 2020-11-11).

EDPB (2020) European Data Protection Board (EDPB) (2020), *Fines proposed for two municipalities*, Press Release, 10. March 2020 (retrieved from https://edpb.europa.eu/news/national-news/2020/fines-proposed-two-municipalities_en on 2020-11-09)

European Commission (2020) European Commission (2020), *The European Cybersecurity Certification Group*, last updated 23. November 2020 (retrieved from https://ec.europa.eu/digital-single-market/en/european-cybersecurity-certification-group on 2020-11-25).

Greenwald (2014) Glenn Greenwald (2014), *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*, New York: Metropolitan Books.

Harbo (2010) Harbo, Tor-Inge (2010), 'The Function of the Proportionality Principle in EU Law', *European Law Journal* 16 (2), pp. 158-185.

Harris and Maymi (2018) Harris, Shon and Fernando Maymi (2018), *CISSP All-in-One Exam Guide*, 8th Edition, McGraw-Hill.

Kuner et al. (2020) Kuner, Christopher, Lee A. Bygrave, Christopher Docksey, Laure Drechsler (eds.) (2020), *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford: Oxford University Press.

Leyden (2017) Leyden, John (2017), 'We need to talk about mathematical backdoors in encryption algorithms', *The Register*, 15. December 2017 (retrieved from https://www.theregister.com/2017/12/15/crypto_mathematical_backdoors/ on 2020-11-25).

Markopouloua et al. (2019) Markopouloua, Dimitra, Vagelis Papakonstantinoua and Paul de Hert (2019), 'The new EU cybersecurity framework: The NIS

Directive, ENISA's role and the General Data Protection Regulation', *Computer Law & Security Review* 35 (6), pp. 1-11.

McCarthy (2020) McCarthy, Kieren (2020), 'Zoom's end-to-end encryption isn't actually end-to-end at all', *The Register*, 1. April 2020 (retrieved from https://www.theregister.com/2020/04/01/zoom_spotlight/ on 2020-11-25).

Michels and Walden (2020) Michels, Johan David and Ian Walden (2020), 'Beyond "complacency and panic": will the NIS Directive improve the cybersecurity of critical national infrastructure?', *European Law Review* 45 (1), pp. 25-47.

Paar and Pelzl (2010) Paar, Christof and Jan Pelzl (2010), *Understanding cryptography. A textbook for students and practitioners*, Heidelberg: Springer.

Oxford Dictionary of English (2015) Stevenson, Angus (2015), *Oxford Dictionary of English*, 3rd edition, Oxford: Oxford University Press.

Soesanto (2018) Soesanto, Stefan (2018), *No middle ground: Moving on from the crypto wars*, Policy Brief, European Council on Foreign Relations (ECFR/263), July 2018.

Voigt and von dem Bussche (2017) Voigt, Paul and Axel von dem Bussche (2017), *The EU General Data Protection Regulation (GDPR). A Practical Guide*, Cham: Springer International Publishing.

Wang (2020) Wang, Yaqiu (2020), 'In China, the "Great Firewall" Is Changing a Generation', *Politico*, 1. September 2020 (retrieved from https://www.politico.com/news/magazine/2020/09/01/china-great-firewall-generation-405385 on 2020-11-25).

8 Abbreviations

AES	Advanced Encryption Standard
CFCS	Center for cybersikkerhed [Centre for Cybersecurity] (DK)
CNIL	Commission Nationale Informatique & Libertés (the French DPA)
DES	Data Encryption Standard
DPA	Data Protection Authority
DPD	Data Protection Directive (1995)
EDPB	European Data Protection Board
EEA	European Economic Area
ENISA	European Union Agency for Cybersecurity (formerly European Network and Information Security Agency)
EPC	European Payments Council
FIPS	Federal Information Processing Standards
GDPR	General Data Protection Regulation
ICO	Information Commissioner's Office (the UK DPA)
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
MAC	Message Authentication Code
NCSC	National Cybersecurity Centre
NIS	(The) Network and Information Systems (Directive)
NIST	National Institute of Standards and Technology
NSM	Nasjonal Sikkerhetsmyndighet [Norwegian National Security Authority]

NOU	Norsk offentlig utredning [Official Norwegian Report]
RFC	Request for Comments
RSA	Rivest–Shamir–Adleman