Disclaimer

Statement for open documents

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 780108. Any dissemination of results here presented reflects only the consortium view.

FENTEC

D3.2 Legal requirement analysis report

Document Identification			
Status	Final	**Due Date**	31/12/2018
Version	1.0	**Submission Date**	14/12/2018

Related WP	WP3	**Document Reference**	D3.2
Related Deliverable(s)	D3.3, D3.4	**Dissemination Level (*)**	PU
Lead Participant	KU Leuven	**Lead Author**	Danaja Fabcic Povse, Wim Vandevelde
Contributors	Anton Vedder, Elisabetta Biasin (KU Leuven), Francisco Gala (ATOS)	**Reviewers**	Jolanda Modic (XLAB)
			Diego Esteban (ATOS)

Keywords:
Legal requirements, legislation, regulation, GDPR, encryption, security of personal data, data protection and privacy by design

Document Information

List of Contributors	
Name	Partner
Danaja Fabcic Povse	KU Leuven-CITIP
Wim Vandevelde	KU Leuven-CITIP
Elisabetta Biasin	KU Leuven-CITIP
Francisco Gala	ATOS

Document History			
Version	Date	Change editors	Changes
0.1	24/07/2018	KU Leuven-CITIP	ToC
0.2	31/10/2018	ATOS	Input on dual use/misuse
0.3	05/12/2018	KU Leuven-CITIP	Final draft
0.4	13/12/2018	KU Leuven-CITIP	Small changes after revision
1.0	14/12/2018	ATOS	Final version for submitting

Quality Control		
Role	Who (Partner short name)	Approval Date
Deliverable leader	Danaja Fabcic Povse (KU Leuven)	14/12/2018
Technical Manager	Michel Abdalla (ENS)	14/12/2018
Quality Manager	Diego Esteban (ATOS)	14/12/2018
Project Coordinator	Francisco Gala (ATOS)	14/12/2018

Table of Contents

List of Tables

List of Figures

List of Acronyms

Abbreviation / acronym	Description
AES	Advanced Encryption Standard
AMLD	Anti-Money Laundering Directive
API	Application programming interface
CCTV	Closed-circuit television
CSDP	Common Security and Defence Policy
CFREU	Charter of Fundamental Rights of the European Union
CSIRTs	Computer Security Incident Response Teams
DPIA	Data Protection Impact Assessment
EB	(FENTEC) Executive Board
EC	European Commission
ECHR	European Convention on Human Rights
EDPS	European Data Protection Supervisor
ENISA	European Union Agency for Network and Information Security
EMD2	Second E-money Directive
EU	European Union
EUGEA	Union General Export Authorization
E-money	Electronic money
FE	Functional Encryption
FIU	Financial Intelligence Unit
GDPR	General Data Protection Regulation
GEA	Global Export Authorization
ICO	Information Commissioner's Office
IEA	Individual Export Authorization
IoT	Internet of Things
ITT	Intangible Technology Transfer
NDA	Non-Disclosure Agreement
NGEA	National General Export Authorization
NIS	Network and Information Security
PAB	Project Advisory Board
PSD1	First payment Services Directive

Abbreviation / acronym	Description
PSD2	Second Payment Services Directive
PSP	Payment Service Provider
WP*x*	Work Package *(number)*

Executive Summary

This deliverable represents the outcomes of the work carried out under T3.2 (WP3) – 'Applicable ethical & legal framework and principles'.

The scope of this Deliverable is twofold.

Firstly, it lays down the ethical and legal framework applicable to FENTEC project, such as the General Data Protection Regulation (GDPR), as well as field-specific regulation; inter alia, the Network and Information Systems Security Directive (NIS directive), Anti-Money Laundering Directive (AMLD), Payment Services Providers Directive (PSD2) and national legislation, e.g. the Belgian camera law.

Secondly, it provides the necessary legal and ethical framework for future work, both in WP3 – 'Requirements and Legal Management', and in the FENTEC research in general.

1 Introduction

1.1 Purpose of the document

Deliverable D3.2 'Legal Requirement Analysis Report' reports on the outcomes of T 3.2 'Applicable ethical & legal framework and principles'.

This report lays out the relevant and applicable ethical and legal framework and principles. The applicable frameworks are identified and further analyzed to ensure that the developed encryption technologies are suited to be used in the areas of the three FENTEC use cases. The task focuses on the extent to which privacy, data protection and cybersecurity legislation applies to the use of new functional encryption technologies as developed through the FENTEC project. The implementation of such new technologies raises questions on the issues of privacy by design, data confidentiality, access control and security standards, meaning that compliance must be achieved with a number of legal instruments. The General Data Protection Regulation (GDPR) [EU2016/679] lays down the main principles of privacy and data protection, while sector-specific legislation is considered in light of the use cases. Sector-specific regulation includes the Anti-Money Laundering [EU2015/849] and Payment Services Directives [EU2015/2366] for the application of the encryption technologies in the area of digital currencies, as well as the European Cybersecurity Strategy for the area of IoT. To the extent necessary, the Directives on E-Privacy [EU2002/58/EC] and E-Commerce [EU2000/31/EC] are taken into account for the anonymous data collection processes in client software, as well as relevant Regulations on combating tax fraud for possible application of the technologies in the field of taxation and government [EC2010/904]. In addition to the abovementioned legislation, the report focuses on the opinions, guidelines and reports published by data protection authorities and interpretative bodies such as the Working Party 29 (WP29), European Data Protection Supervisor (EDPS) and European Union Agency for Network and Information Security (ENISA). Moreover, this analysis includes documents such as the ENISA Opinion Paper on Encryption and the UNESCO report on Encryption and Human Rights.

Moreover, ethical issues are identified. In particular, the deliverable focuses on dual use and misuse of functional encryption technologies. In this regard, we provide legal and ethical guidelines, as well as relevant practical rules by which all FENTEC partners are to abide.

Lastly, this deliverable provides high level guidelines on how compliance can be realized and risks may be mitigated in order to ensure that fundamental principles are accounted for the *privacy by design methodology.*

1.2 Structure of the document

This document is structured as follows:

- Section 2 'Applicable ethical and legal framework – general overview' discusses data protection and privacy rules in Europe

  Encryption is an important tool to increase privacy and security in data processing and (online) privacy. In this section, the General Data Protection Regulation (GDPR), Convention 108 of the Council of Europe, and certain non-binding documents, such as expert opinions and white papers are discussed.
- Section 3 Misuse and dual use of FENTEC research

Functional encryption can be used for military purposes (dual use) or by criminals (misuse). This section lays down measures the consortium is taking to prevent dual and misuse of FENTEC technologies.

- The next three sections focus on FENTEC use cases
  In these three sections, the FENTEC use cases are discussed. Since different legislation applies to different use cases (for example, anti-money laundering rules apply to the digital currency scenario, whereas the eprivacy directive applies to the anonymous Amazon data collection).

Furthermore, brief overview of future work as well as a high-level overview of privacy by design methodology and a GDPR one-pager are presented.

2 Applicable ethical and legal framework – general overview

2.1 Privacy and data protection in Europe

This section will lay out the main regulatory instruments, applicable to encryption under the data protection and privacy regime in Europe. While privacy and data protection are often mentioned together or interchangeably, they fall under different legal regimes and requirements. Nonetheless, these regimes often overlap.

Privacy and data protection are both **fundamental rights**. While the former is protected under Article 8 of the European Convention on Human Rights (ECHR)[1] and Article 7 of the Charter of Fundamental Rights of the European Union (CFREU)[2], the latter has no direct counterpart in the ECHR but is enshrined in Article 8 of the CFREU. Two systems therefore ensure the protection of privacy and data protection in Europe.[3]

Article 8 of the ECHR protects the private and family life, the home and correspondence of an individual:

> **Right to respect for private and family life**
>
> 1. Everyone has the right to respect for his private and family life, his home and his correspondence.
>
> 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Similarly, Article 7 of the CFREU:

> **Respect for private and family life**
>
> Everyone has the right to respect for his or her private and family life, home and communications.

Article 52/1 of the CFREU provides for exceptions. A limitation of a right is only permitted if it meets the criteria, laid down in this paragraph ('proportionality test'):

> **Scope and interpretation of rights and principles**
>
> 1. Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.

[1] Charter of Fundamental Rights of the European Union, *O.J.E.U*, 18 December 2000, C 364/01.
[2] Charter of Fundamental Rights of the European Union, *O.J.E.U*, 18 December 2000, C 364/01.
[3] Juliane Kokott and Christoph Sobotta, 'The Disctinction between privacy and Data Protection in the Jurisprodence of the CJEU and the ECtHR' (2013) 3 Internaitonal Data Privacy Law 222, 22.

The two regimes have a slightly different scope of application. The ECHR applies to states signatories, who are members of the Council of Europe, an international organisation spanning 52 countries within the geographical Europe. Any individual whose convention rights had been violated can file a complaint with the European court of human rights, the authoritative interpreter body of the Convention. On the other hand, the CFREU applies to institutions of the European Union and to the 28 member states when they are implementing EU law.

Nevertheless, the two regimes are intertwined. First, Article 52(3) CFREU states that '*in so far as this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention'*. In other words, when both the ECHR and the CFREU contain corresponding rights – which appears to be the case for privacy at least, and data protection to a certain extent – the interpretation of the CJEU should follow the ECtHR's. Second, the ECtHR extends the protection afforded by Article 8 ECHR for private life to personal data. There is a nexus between privacy and data protection: private life considerations can arise from compiling data on a particular individual.[4] [5] .Third, the CJEU often fails to distinguish between privacy and data protection in its reasoning.[6]

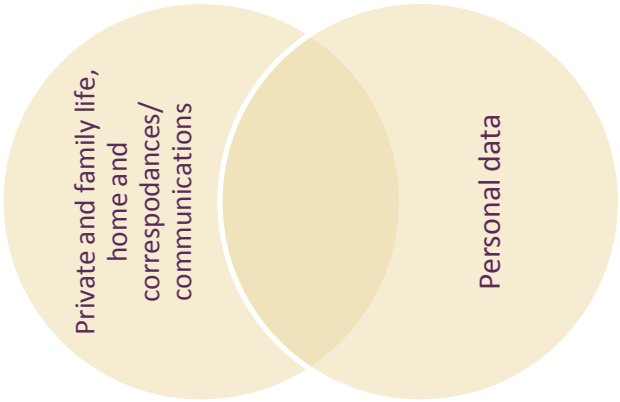

Figure 1: the overlap between the concepts of privacy and data protection

The right to data protection, on the other hand, is contained in Art. 8 of the CFREU, and in secondary legislation on EU level. Until 25 May 2018, that was the Directive 95/46/EC (Data Protection Directive); from that date on, the new Regulation 679/2016 (General Data Protection Regulation, GDPR) has replaced it wholly. The Directive 680/2016 (The Law Enforcement Directive) applies to data processing by law enforcement authorities, such as the police and courts.

Moreover, the right to data protection is also laid down in Convention no. 108 of the Council of Europe, as well as in some non-binding documents, such as recommendations and white papers, which we will explain in more detail below in this section.

How do privacy and data protection relate to encryption?

Encryption contributes to privacy of communications, since it renders them unintelligible to anyone who does not possess the decryption key. It can keep information, that would otherwise be accessible to a large number of persons, restricted only to those who can decrypt it. Similarly, encrypting personal data

[4] Factsheet, Personal data protection, https://www.echr.coe.int/Documents/FS_Data_ENG.pdf.
[5] Benedik vs. Slovenia
[6] On the entanglement between the notions of privacy and data protection, see Gloria Gonzalez Fuster, 'Conclusions', in *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Law, Governance and Technology Series (Springer, Cham, 2014), 268-71.

can mask them to persons without the decryption key, rendering them pseudonymous data (but not anonymous data, on principle), and increasing the security of their processing.

2.1.1 General Data Protection Regulation

In the GDPR, encryption plays a double role. On the one hand, encrypting personal data has implications for GDPR's applicability, on the other hand, encryption is a security measure that contributes to security of personal data.

The General Data Protection Regulation (GDPR)[7] entered into force on May 25 2018, wholly replacing and repealing the old regime under the Data protection directive.

2.1.1.1 When and to whom does the GDPR apply in FENTEC?

The GDPR applies to processing of personal data. They are defined in Art. 4(1) and (2), respectively as:

'**personal data**' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

'**processing**' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

There are three types of data, relevant for GDPR scope of application:

1. Personal data
2. Pseudonymised data
3. Anonymised data

[7] General Data Protection Regulation.

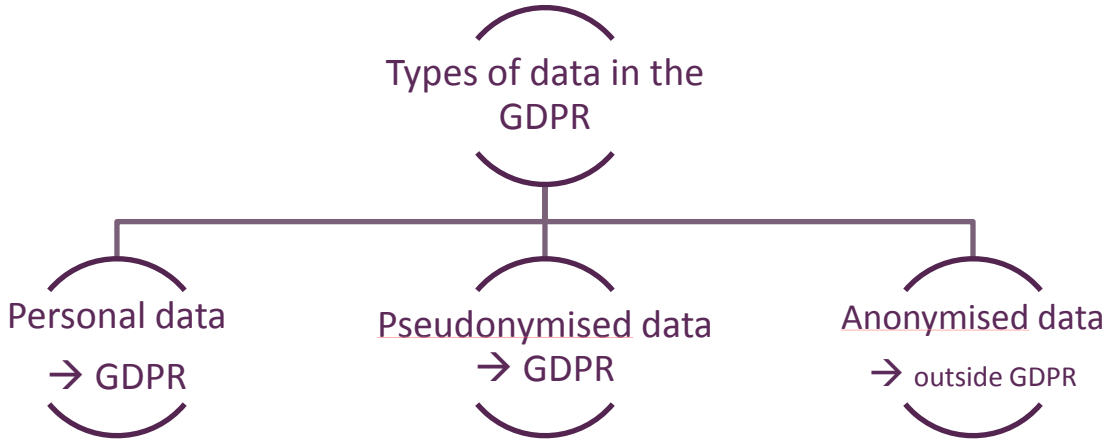

Figure 2: types of data in the GDPR

The GDPR applies to the first two categories, but it does not apply to data that have been wholly anonymised. This means that an individual cannot be singled out anymore, records relating to an individual cannot be linked, and information concerning an individual cannot be inferred.[8] Data that do not meet this requirement, are considered personal data.

Pseudonymised data still fall under the GDPR. They are data that have been processed in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person, according to Art. 4(5) of the GDPR.

It is essential that the additional information, needed for attribution, is kept separately from the personal data themselves. How likely is a third party to get that extra information? This is the deciding criterion that delineates pseudonymised data (within the scope of the GDPR) and anonymised data (outside the scope of the GDPR).[9] The question was answered by the Court of Justice of the European Union in the Patrick Breyer case.[10] In this case, the court had to rule on whether dynamic IP addresses, which in itself cannot be attributed to an individual, are personal data. According to the Court's judgment, para. 49:

> 'a dynamic IP address registered by an online media services provider when a person accesses a website that the provider makes accessible to the public constitutes personal data within the meaning of that provision, in relation to that provider, where the latter has the legal means which enable it to identify the data subject with additional data which the internet service provider has about that person.'

This means that with regards to encrypted data there are two options:

[8] WP29 on anonymization.
[9] Spindler, Schmechel, Personal data and encryption in the European General Data Protection Regulation.
[10] Case C-582/14, Patrick Breyer v. Bundesrepublik Deutschland.

- If the organisation/person, wishing to decrypt the encrypted information or text, **can** obtain the decryption key by lawful means reasonably likely, then the data contained therein are **personal data and the GDPR applies**.
- If the organisation/person, wishing to decrypt the encrypted information or text, **cannot** obtain the decryption key by lawful means reasonably likely, then the data contained therein are **not personal data** (from the point of view of that organisation/person) **and the GDPR does not apply to them**.

Therefore, the key must be kept separate from the encrypted information or text and measures must be put in place in order to prevent unauthorised persons from acquiring it.[11]

The research in FENTEC will not use personal data.

- For the digital currency use-case it is specified that the digital currency system (testing) will use **mock-up data**
- For the IoT smart camera use case it is specified that the testing of IoT use-cases will rely on **fabricated data**
- For the web analytics use case it is specified that an **anonymous data** collection will be created relying on functional encryption in the Amazon AWLESS client: "Using the core results of the FENTEC project, Wallix will use Functional Encryption to encrypt the user data directly on the user device. As only encrypted data will be collected without knowledge of the decryption keys, Wallix will be able to compute statistics over multiple users but will not be able to retrieve or decrypt the data of any single user."

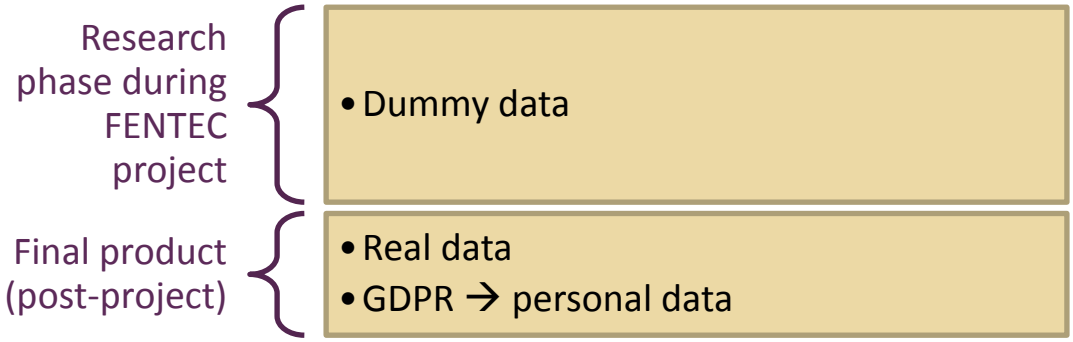

Figure 3: use of personal data in FENTEC

However, when the FENTEC functional encryption technology is eventually implemented and used in real-life apps (in a post-project setting), personal data may well be processed. Somewhere, there is always going to be a **data subject**. Depending on the purpose of the data processing, the legal ground which allows the data processing and several other – case specific or sector specific – parameters, this person will have strong rights: to information, to access, to be forgotten, to review decisions, etc. Therefore, it is important that data protection and privacy safeguards are taken into account from the very beginning of the design process. This is referred to as **privacy by design or data protection by design**.

[11] Nb. The distinction between public and private key cryptography does not have an impact by itself.

2.1.1.2 Data protection/privacy by design and by default

This principle, which is laid out in Art. 25 of the GDPR, entails that: "appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed" are implemented, "That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons."

Article 25(1), which sets out the **data protection by design** obligation, requires that data protection be included from the onset of the designing of systems, rather than as a later addition. The data controller must implement appropriate technical and organisational measures (e.g. pseudonymisation) in order to implement the data protection principles such as data minimisation (only processing data that is necessary for the purpose). Data minimisation applies to amount of data, its period of storage and its accessibility. In particular, it must be ensured that by default personal data are not made accessible to an indefinite number of people.

Article 25(2), which sets out the **data protection by default** obligation, requires the controller to implement appropriate technical and organisational measures, which ensure that by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, those measures must ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

The specific obligation for the data controller is therefore to adopt measures, which implement data protection principles: lawfulness of processing, data minimisation, purpose limitation, storage limitation and integrity and confidentiality. In this manner, the controller can demonstrate compliance and adherence to the accountability principle, according to Art. 5(2).

GDPR suggests the adoption of the following measures, which contribute to privacy by design: minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing and enabling the controller to create and improve security features, according to Recital 78 of the GDPR.

On the premise that the processing personal data partially or completely supported by IT systems should always be the outcome of a design project, Data Protection By Design requires the controller to embed safeguards and mechanisms throughout the lifecycle of the application/service/product to protect the right to data protection of the data subject; whereas Data Protection by Default requires the activation and application of such safeguards as default settings.

Data protection by design is conceptually similar to the idea of privacy by design – the difference being that they focus on data protection and privacy, respectively. The Court of Justice of the European Union seems to treat the right to privacy and the right to data protection as two sides of the same coin,[12] so it is reasonable to assume that the tenets of privacy by design also apply to Article 25.

[12] Joined Cases C-468/10 and C-469/10, ASNEF and FECEMD v. Administración del Estado, 24 November 2011; *and* Joined Cases C-92/09 and C-93/09, Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen: the Court deals with them together, without clearly delineating one right from another.

A privacy-by-design compliant system follows three privacy-specific protection goals: *unlinkability*, *transparency*, and *intervenability*, and three security-specific goals: *confidentiality*, *integrity*, and *availability* (also referred to as CIA).[13]

Privacy by design consists of two main elements: **incorporating substantive privacy protections** into an organisation's practice and **keeping up comprehensive data management procedures** during the life cycle of a service or product.[14]

In May 2018, the EDPS (European Data Protection Supervisor) issued a Preliminary Opinion on Privacy by Design, aiming to provide guidance to controllers and processors for the implementation of the principle.[15] The Preliminary Opinion further describes the key aspects of Data Protection by Design and outlines three possible steps for the operationalisation thereof. These are:

1. The definition of a methodology to integrate privacy and data protection objectives as part of projects implying the processing of personal data;
2. The identification and implementation of adequate technical and organisational measures to be integrated in those processes;
3. The integration of the support for privacy within organisations through the definition of tasks and allocation of resources and responsibilities.

Data Protection by Design constitutes a new requirement but it is not a new concept for the data protection legal framework. The ethical, legal and functional requirements, as well as a set of measures and controls to be implemented into the final product must be defined early in the design process in order to meet the requirement.

The key is therefore to focus on both legal compliance and on risks from computer engineering point-of-view. It is especially important that privacy by design is not understood as solely an IT solution to the privacy risks, but also in a processual manner, encompassing compliance, computer engineering, business and organisational processes.[16]

The legal obligation of data protection/privacy by design can be broken down schematically.

[13] EDPS – Privacy by design.
[14] ENISA, Privacy and Data Protection by Design – from policy to engineering, December 2014.
[15] EDPS – Privacy by design.
[16] Regulating privacy by design (privacy enhancing technologies (Technology: Transforming the Regulatory Endeavor, Rubinstein, Ira S., Berkeley Technology Law Journal, Summer, 2011, Vol. 26 (3).

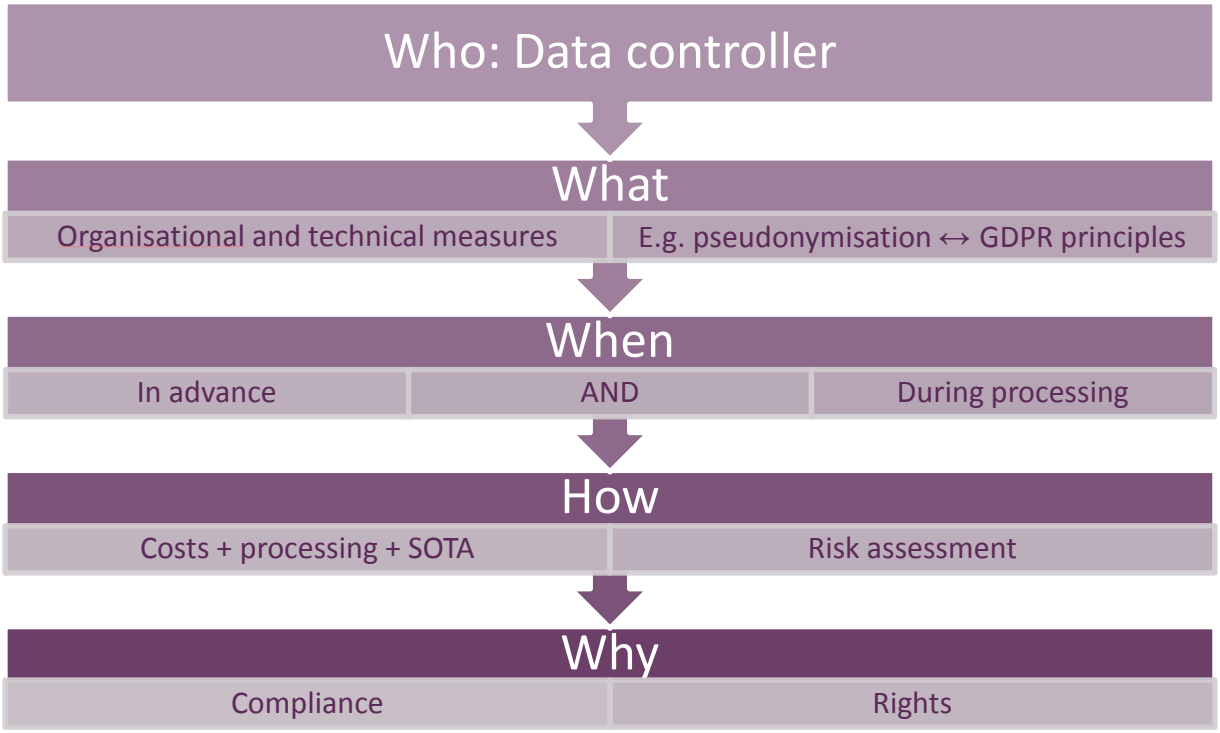

Figure 4: Data protection/privacy by design requirement

We provide guidelines on implementation in Annex II: Privacy by design methodology. It is based on state of the art academic literature[17] [18] as well as work, carried out in previous and current projects in which KU Leuven-Centre for IT & IP law has been involved, e.g. WITDOM,[19] DOGANA,[20] PDP4E,[21] PRISE.[22]

2.1.1.3 Security requirements

Encryption, apart from masking data through pseudonymisation or anonymisation, can also contribute to security of processing. Art. 32 of the GDPR requires the data controller and the data processor to **implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.**[23] In laying down these measures, they must take into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the

[17] Transparency in the design process, https://link.springer.com/chapter/10.1007/978-3-319-22906-5_15.
[18] Privacy enhancing and transparency enhancing technologies, https://link.springer.com/chapter/10.1007/978-3-319-55783-0_3.
[19] www.witdom.eu
[20] www.dogana-project.eu
[21] www.pdp4e-project.eu
[22] https://www.law.kuleuven.be/citip/en/research/projects/ongoing/prise
[23] The data controller and the data processor are organisations, involved in the processing.
The data controller is the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. If the means and purposes of processing are set out in EU or national law, then such law also determines the controller or the specific criteria for its nomination. (Art. 4(7) of the GDPR)
The data processor is a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller (Art 4(8) of the GDPR).

risk of varying likelihood and severity for the rights and freedoms of natural persons. The main risks, that an organization is likely to face, are accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

The GDPR suggests the following security measures; however, the list is not complete.

(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.

Somewhat inconsistently, the GDPR refers to encryption and pseudonymisation as two equal measures, even though that may not be the relation between them, as explained above.

Moreover, the data controller must also put in place **a mechanism to notify** the competent data protection authority as well as the data subject in case of a personal data breach, i.e. a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

2.1.1.4 Data Protection Impact Assessment (DPIA)

The GDPR lays down very high fines for non-compliance (see its Art. 83 and 84). In order to demonstrate accountability and compliance, a **data protection impact assessment** (DPIA) can be drafted. A DPIA can enhance compliance where processing operations are likely to result in a high risk to the rights and freedoms of natural persons; in other words, it is a process for building and demonstrating compliance[24]. It is a useful tool to identify, assess and manage risks to individuals' rights and freedoms. In line with the GDPR's notion of decreasing administrative burdens, it replaces the former directive's Art. 18 notifications to competent authorities. It is a type of self-assessment instead of notification of authorities about processing. Nonetheless, in some cases a prior consultation with the authorities is still necessary, according to Art. 36. The minimum content of a DPIA is laid down in the GDPR:

- a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;
- an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
- an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph;
- the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the GDPR taking into account the rights and legitimate interests of data subjects and other persons concerned.

A DPIA will be drafted by the FENTEC consortium during the design phase in order to facilitate future compliance, taking into account the development of project works, including the encryption technologies and different use cases.

[24] WP29 DPIA.

2.1.2 Convention 108

Convention no. 108, adopted by the Council of Europe[25], is an international law instrument, which protects an individual's right to privacy, with regard to automatic processing of personal data relating to him ("data protection"). It applies to automated personal data files and automatic processing of personal data in the public and private sectors. It defines the terms as following:

'Personal data' means any information relating to an identified or identifiable individual ('data subject'). 'Automated data file' means any set of data undergoing automatic processing. 'Automatic processing' includes the following operations if carried out in whole or in part by automated means: storage of data, carrying out of logical and/or arithmetical operations on those data, their alteration, erasure, retrieval or dissemination. 'Controller of the file' means the natural or legal person, public authority, agency or any other body who is competent according to the national law to decide what should be the purpose of the automated data file, which categories of personal data should be stored and which operations should be applied to them. Unlike the GDPR, it does not define the term 'processor', implying that it does not apply to them, and that it only applies to data controllers.

The Convention lays down basic principles of data protection, such as quality of data (similar to data principles, contained in Art. 5 of the GDPR), the prohibition of processing of special categories of data, i.e. those revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, and personal data relating to criminal convictions. It also lays down basic security principles and grants the data subject certain rights, such as the right to access and information about processing, the right of erasure, and the right to an effective remedy against violations.

The Convention also contains some rules on cross-border transfers of personal data; in such cases, both states must provide for data protection safeguards in their respective legislations.

2.2 Cybersecurity legislation in Europe

2.2.1 The 2013 EU cybersecurity strategy

In 2013, the European Commission (EC) released its European Cybersecurity Strategy[26] as part of the Digital Agenda for Europe. This strategy, named "*An Open, Safe and Secure Cyberspace*", aims to protect fundamental rights, democracy, and the rule of law in cyberspace in order to secure freedom online. However, this goal can only be achieved when safety and security are taken into account. Furthermore, the success of the Digital Single Market and new technologies rely on the trust and confidence of its users, which requires a high level of safety and security in the online environment.

The threat of large-scale cybersecurity incidents with widespread effects only increases with the expansion of the Internet of Things (IoT). This makes cybersecurity an important global issue for both the private and public sector. On the one hand, it is up to governments on the European and national level to formulate rules and requirements for transparency, accountability, and security. On the other hand, it is the industry that owns and operates significant parts of cyberspace. Consequently, they should continue to play a leading role in the management of cyberspace.

[25] Convention 108.
[26] Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, 7 February 2013, JOIN(2013) 1 final.

The 2013 EU cybersecurity strategy sets out several principles for cybersecurity which should guide cybersecurity policy in the EU. One of these principles establishes a shared responsibility between all relevant actors to ensure and strengthen cybersecurity. The cybersecurity strategy also proposes five strategic priorities, which include actions to be taken by the private sector:

1. **Achieving cyber resilience**

For this goal, the Commission asks the industry to "*take leadership in investing in a **high level of cybersecurity and develop best practices and information sharing** at sector level and with public authorities with the view of ensuring a strong and effective protection of assets and individuals, in particular through public-private partnerships like EP3R an TDL*"[27] and to "*promote **cybersecurity awareness at all levels**, both in business practices and in the interface with customers. In particular, industry should reflect on ways to make CEOs and Boards more accountable for ensuring cybersecurity*"[28].
The Commission also calls for the swift adoption of the proposal for a Directive on a common high level of Network and Information Security (NIS) across the Union, which will be discussed below.

2. **Drastically reducing cybercrime**

3. **Developing cyberdefence policy and capabilities related to the Common Security and Defence Policy (CSDP)**

4. **Develop the industrial and technological resources for cybersecurity**

Here, the Commission invites public and private stakeholders to "*stimulate the development and adoption of **industry-led security standards**, technical norms and security-by-design and privacy-by-design principles by ICT product manufacturers and service providers, including cloud providers; new generations of software and hardware should be equipped with stronger, embedded and user-friendly security features"*[29] and to *"develop industry-led standards for companies' performance on cybersecurity and improve the information available to the public by developing security labels or kite marks helping the consumer navigate the market"*[30].

5. **Establish a coherent international cyberspace policy for the European Union and promote core EU values**

The relevance of the 2013 EU cybersecurity strategy for FENTEC is limited to the abovementioned references to the private sector. The functional encryption technology developed under FENTEC contributes to increased cyber resilience and a higher level of cybersecurity in the EU. Functional encryption should be integrated into a wide range of ICT applications and services instead of classical encryption techniques. This way, functional encryption will become an accepted security standard on its own.

[27] *Ibid.*, 7.
[28] *Ibid.*, 8-9.
[29] *Ibid.*, 13.
[30] *Ibid.*

2.2.2 The Network and Information Systems Directive (2016/1148)

2.2.2.1 Introduction

The Network and Information Systems (NIS) Directive[31] entered into force on 8 August 2016 and Member States had until 8 May 2018 to transpose the Directive into national law. It aims to increase the overall level of cybersecurity in the EU by developing a common approach and coordinating Member States' actions. To achieve this goal, the directive imposes obligations on both Member States and the private sector. The Directive aims at minimum harmonization, leaving it up to the Member States to adopt or maintain stricter rules to ensure a higher level of security of network and information systems.[32] It also mentions that sector-specific EU legislation may already establish rules concerning the security of network and information systems. The provision of those legal acts should nevertheless apply where they provide for requirements that are at least equivalent in effect to the requirements of the NIS Directive.[33]

2.2.2.2 Subject matter and scope

Definitions

The NIS Directive defines *'network and information system'* as:

a) "*an electronic communications network within the meaning of point (a) of Article 2 of Directive 2002/21/EC*[34]*;*

b) any device or group of interconnected or related devices, one or more of which, pursuant to a program, perform automatic processing of digital data; or

c) digital data stored, processed, retrieved or transmitted by elements covered under points (a) and (b) for the purposes of their operation, use, protection and maintenance."[35]

The *'security of network and information systems'* refers to "*the ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems.*"[36]

Obligations for Member States

Under the Directive, Member States must; adopt national strategies on the security of network and information systems, designate one or more national competent authorities to monitor the application of the NIS Directive, designate a single point of contact that has a liaison function to ensure cross-border

[31] 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.
[32] Article 3 of Directive (EU) 2016/1148.
[33] Recital 9 and article 1, 7 of Directive (EU) 2016/1148.
[34] Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive), OJ L 108, 24 April 2002, p. 33–50, according to article 2 (a): *electronic communications network means transmission systems and, where applicable, switching or routing equipment and other resources which permit the conveyance of signals by wire, by radio, by optical or by other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including Internet) and mobile terrestrial networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed*.
[35] Article 4, (1) of Directive (EU) 2016/1148.
[36] Article 4, (2) of Directive (EU) 2016/1148.

cooperation, and designate one or more Computer Security Incident Response Teams (CSIRTs) tasked with risk and incident handling.[37]

Obligations for the private sector

The Directive also contains obligations for the private sector. 'Operators of essential services' and 'digital service providers' are subject to safety and incident notification requirements under Chapter IV and V respectively.

1. Operators of essential services

An *'operator of essential services'* means "*a public or private entity of a type referred to in Annex II, which meets the criteria laid down in Article 5 (2).*"[38] Essential services refer to the sectors of energy, transport, banking, financial market infrastructures, health, drinking water supply and distribution, and digital infrastructure.[39] Article 5, 2 sets out the following three criteria which operators of essential services must fulfill:

a) an entity provides a service which is essential for the maintenance of **critical societal and/or economic activities**;

b) the provision of that service **depends on network and information systems**; and

c) an incident would have **significant disruptive effects** on the provision of that service.

Member States have until 9 November 2018 to identify the operators of essential services with an establishment on their territory.[40] Additionally, it is up to the Member States to determine the significance of a disruptive effect as referred to in Article 5, 2 (c). This assessment must take several cross-sectoral factors into account, as laid down by Article 6.

Operators of essential services must take appropriate and proportionate technical and organizational measures to manage risks and to prevent and minimize the impact of incidents.[41] They must also notify, without undue delay, the competent authority or the CSIRT of incidents that have a *significant impact* on the continuity of the provided essential services.[42] The specific substance of these obligations is defined under national law.

2. Digital service providers

A *'digital service provider'* is "*any legal person that provides a digital service*"[43] Such a digital service is either (1) an online marketplace, (2) an online search engine, or (3) a cloud computing service.[44]

Under Chapter V, these digital service providers have similar obligations to the operators of essential services. They must also identify and take appropriate and proportional technical and organizational measures to manage risks and to prevent and minimize the impact of incidents.[45] The notification requirement also applies to digital service providers. They must notify the competent authority or the

[37] Article 1, 2 (a) and (e), article 8, and article 9 of Directive (EU) 2016/1148.
[38] Article 4, (4) of Directive (EU) 2016/1148.
[39] Annex II of Directive (EU) 2016/1148.
[40] Article 5, 1 of Directive (EU) 2016/1148.
[41] Article 14, 1 and 2 of Directive (EU) 2016/1148.
[42] Article 14, 3 of Directive (EU) 2016/1148.
[43] Article 4, (6) of Directive (EU) 2016/1148.
[44] Annex III of Directive (EU) 2016/1148.
[45] Article 16, 1 and 2 of Directive (EU) 2016/1148.

CSIRT without undue delay of incidents that have a *substantial impact* on the provision of the digital service offered in the EU.[46]

The obligations of the NIS Directive are relevant for FENTEC to the extent that implementers of the technology are identified as essential service providers or digital service providers. Functional encryption technology could be an appropriate technical measure to manage risks and to prevent and minimize the impact of incidents, thereby contributing to compliance with the directive. Examples are energy suppliers or distributors in case of smart meters, or cloud computing services such as Amazon Web Services.

2.2.3 The 2017 cybersecurity package

In 2017, the EC published a Joint Communication on "*Resilience, Deterrence and Defence: Building strong cybersecurity for the EU*".[47] This cybersecurity package builds on what already exists, but also introduces new initiatives in order to improve the overall level of cybersecurity in the EU.

The EC observes that cybersecurity risks are increasing at an incredibly high rate. Billions of devices are becoming interconnected and part of the IoT through network integration, often controlling essential and critical infrastructures (e.g. energy, banking, transport). In order to protect these devices, and consequently ourselves, cybersecurity should be a priority from the very beginning. This cybersecurity package aims to move from a reactive to proactive approach by involving all relevant actors on the EU, Member State, industry, and individual levels.

One important initiative is the proposal for a reform of ENISA by giving it a permanent mandate and more resources. The goal is to allow ENISA to provide better support to Member States, EU institutions, and the industry in crucial areas such as the implementation of the NIS Directive. *Another key initiative* is the proposal for a voluntary EU cybersecurity certification framework. This framework allows ICT products, services, and/or systems to be evaluated against a common set of clearly defined security standards. An EU-wide cybersecurity certification scheme would benefit the integration of high resilience standards into ICT products on the EU market. It also limits the fragmentation of national certification schemes across the EU while strengthening the concept of 'security by design'. The EC identifies three key areas for relevant stakeholders in this area: security in critical or high-risk applications (e.g. cars, power plants, medical devices), cybersecurity in widely-deployed security tools (e.g. encryption), and security by design for IoT devices. Both of these initiatives were adopted in the proposal for a "Cybersecurity Act"[48], as part of the 2017 cybersecurity package.

The Joint Communication also mentions the importance of encryption of products and services used within the Digital Single Market. Strong encryption is essential for secure digital identification systems, but also protects intellectual property and fundamental rights, and ensures the safety of online commerce.

[46] Article 16, 3 of Directive (EU) 2016/1148.
[47] Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, 13 September 2017, JOIN(2017) 450 final.
[48] Proposal for a Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act"), 13 September 2017, COM(2017) 477 final.

2.3 Relevant non-binding rules on encryption (soft law)

2.3.1 OECD: Guidelines for cryptography policy

OECD, the Organisation for Economic Cooperation and Development, adopted its Recommendation concerning Guidelines for cryptography policy on 27 March 1997. The Guidelines address policy-makers with the goal of decreasing obstacles in international trade and evolution of information and communication networks by reducing policy disparities. Like the GDPR, they link cryptography to privacy and data protection on the one hand, and to security of information systems on the other. They specifically mention the use of cryptography by the government, and its use in digital signatures and electronic payments. Any national restrictions on the use of cryptography must be reported to the organisation.

While the Guidelines mainly address governments, they can be taken into account by both the public and the private sector when designing cryptography-based products.

Eight principles should be taken into account when regulating cryptographic methods:

1. User trust: using encrypted communications can help foster trust by the users of ICTs, particularly in electronic commerce and electronic payment systems.
2. User choice: governments should on principle not regulate which specific methods should be used for cryptography. Since different threats and risks exist, each user should be free to choose the most appropriate type of cryptography regarding key management system, public or private key, etc.
3. Market-driven development: bottom-up creation of cryptography methods rather than top-down. Development is based on market demand rather than government-imposed requirements.
4. Standardisation: a voluntary adherence-based system through market forces, international or national standard setting organisations.
5. Privacy and data protection: cryptography can ensure confidentiality of information and communication as well as contribute to privacy of transactions by masking one's identity.
6. Lawful Access of law enforcement to encrypted information may sometimes be necessary, either by accessing stored information and/or intercepting communication. Some countries provide for storage of decryption keys by trusted keyholders (as a kind of a public escrow); however, the need to access keys and decrypt information must be balanced against the principles of proportionality and necessity.
7. Liability: rules must be laid down regarding liability in case of a breach
8. International cooperation: national legal regimes are border-bound, while information is not and flows freely between territories. Incompatibilities may lead to use of several products with the aim of compliance, where one might have sufficed if the policies were aligned.

2.3.2 ENISA: Opinion paper on encryption

The Opinion paper on encryption: strong encryption safeguards our digital identity[49] by ENISA (European Union Agency for Network and Information Security) focuses on cryptography in the context of potentially reducing strong encryption for law enforcement and intelligence services. It argues strongly against backdooring due to its past ineffectiveness. Its key messages are:

[49] ENISA opinion paper on encryption.

1. Backdoors are not a solution, since they put legitimate users at risk by the virtue of its existence and punish the wrong people.
2. Backdoors are ineffective against criminals since the latter can develop their own cryptographic tools.
3. Regulation is always behind the latest technology – law enforcement can be effective without the use of backdoors and key escrow, and criminals will always find a way around the rules.
4. The emergence of a fully digital society in Europe may be jeopardised by the existence of backdoors and key escrow.
5. Legal controls of cryptography may be harmful to innovation and competitiveness, based on previous experience in the US.

2.3.3 UNESCO: Human rights and encryption

UNESCO's report on Human Rights and Encryption[50] forms part of its publication series on Internet Freedom and focuses on the use of encryption in law and policy as well as specific use cases. Encryption is presented as an important measure, contributing to genuine enjoyment of the freedom of expression online. Moreover, encryption has a strong impact on anonymity, access to information, private communication and privacy. The report builds on OECD guidelines, discussed above.
Its key recommendations are:

1. Encryption should be a part of general internet governance policy.
2. The link between human rights and encryption is a strong one and should be more stressed in public debate in order to strengthen the former. This includes the need to implement safeguards against backdoors, increasing transparency and accountability regarding safeguards in the code, increasing sensitivity to violations of minority rights and rights of vulnerable groups, such as LGBTI groups, girls and women and ethnic and national minorities.
3. Involvement of relevant stakeholders in policy debates: government, industry, civil society.
4. Encryption in itself is a strong contributor to human rights, but it is not a magic button – need to implement and embed other solutions and safeguards as well.

It further lists recommendations for policy makers, intermediaries and platforms, and the civil society and developers. In this regard, this document goes further than the others, since it goes beyond addressing only policy-makers. Here, we summarise the guidelines, applicable to developers, as FENTEC is about developing functional encryption technologies.

1. Make encryption convenient in smart technologies: do not ask users to choose to opt in/opt out of security measures constantly (similar to security by design principle).
2. Users should have a realistic idea of the risks they face without overly burdensome requirements for encryption.
3. Vulnerable groups are especially in need of encryption to protect their human rights.
4. Standardisation to focus on improving protocols, known to be insecure.

[50] UNESCO, Human Rights and Encryption.

3 Misuse and dual use of FENTEC research

3.1 Introduction and problem statement

The functional encryption technology developed within the FENTEC project could potentially be used by military (dual-use) and/or criminal actors (misuse). "Misuse" refers to unethical purposes such as crime, terrorism, surveillance technologies that could curtail human rights and civil liberties, etc.[51] The risk of such dual-use or misuse is, however, relatively low. Functional encryption is very similar to standard encryption; it has virtually the same purpose and value for military and criminal actors. The main differences are its flexibility, efficiency, and the exact way in which it operates. Functional encryption technology within the FENTEC project is being developed exclusively for civilian purposes, with the goal of general availability on the market. Fields of application include Internet of Things (IoT) products, financial services, and data collection through web services. Functional encryption would protect against privacy abuses even more extensively than standard encryption, due to compartmentalization. Dual-use and misuse of the FENTEC results would therefore be of low risk. Despite this, we must still acknowledge and consider these risks by taking all necessary precautionary mitigation measures, laid down in Sections 3.3, 3.4, and 3.5.

3.2 Applicable International and European legislation for dual-use items

The international and European regime for exports of dual-use items aims to secure regional and international security and stability by controlling items that can be used for civil and military purposes.[52] The FENTEC technology could be used for both of these purposes, thus falling under this dual-use regime. On the international level, this is governed by the Wassenaar Arrangement. On the European level, Council Regulation (EC) No 428/2009 and Commission Delegated Regulation (EU) 2015/2420 are of particular relevance.

3.2.1 The Wassenaar Arrangement

The Wassenaar Arrangement is a multilateral export control regime between 42 participating states. These states include, but are not limited to, all EU member states (excluding Cyprus) and Switzerland. The Wassenaar Arrangement has produced common non-binding policies and standards which have been implemented by participating states through domestic law and by the European Union (EU) through Regulation (EC) No 428/2009 and Commission Delegated Regulation (EU) 2015/2420. The Wassenaar policies and standards are used as tools for the interpretation of export control legislation.[53] The Wassenaar Arrangement sets out a joint dual-use control list of designated dual-use items, which was implemented by Commission Delegated Regulation (EU) 2015/2420.[54]

[51] [GUI1] Guidance note — Potential misuse of research. European Commission, http://ec.europa.eu/research/participants/data/ref/h2020/other/hi/guide_research-misuse_en.pdf.
[52] The Wassenaar Arrangement (2018). *About us.* Available: http://www.wassenaar.org/about-us/. Last accessed 18/10/2018.
[53] The Wassenaar Arrangement (2018). *About us.* Available: http://www.wassenaar.org/about-us/. Last accessed 18/10/2018.
[54] The Wassenaar Arrangement (2018). *Control lists.* Available: http://www.wassenaar.org/control-lists/. Last accessed 18/10/2018; Annex I, 3 of Commission Delegated Regulation (EU) 2015/2420.

Due to the implementation into domestic law and EU law, the Wassenaar Arrangement will not be used as a direct reference but rather as a tool for interpretation. For this purpose, the Wassenaar Best practices and guidelines should be taken into account.

3.2.2 Council Regulation (EC) No 428/2009 and Commission Delegated Regulation (EU) 2015/2420

The control of exports of dual-use items in the EU is regulated by Council Regulation (EC) No 428/2009 and by Commission Delegated Regulation (EU) 2015/2420. The latter is an amendment to the former and also implements the current Wassenaar dual-use control list of designated dual-use items. In 2016, the EU has published a proposal for revisions to expand the scope of the current dual-use exports control regime.[55]

Functional encryption technology as developed in the FENTEC project is a form of cryptography and therefore a dual-use item under Annex I, category 5, part 2 of Regulation 428/2009 (as amended by Regulation 2015/2420). The European exports control regime for dual-use items is applicable.

3.2.2.1 Definitions

Dual-use item

Regulation 428/2009 defines '*dual-use item*' as:

> *"... items, including software and technology, which can be used for both civil and military purposes, and shall include all goods which can be used for both non-explosive uses and assisting in any way in the manufacture of nuclear weapons or other nuclear explosive devices;".* [56]

This is a straightforward and clear definition of dual-use items. If it can be used for both civil and military purposes, it can be classified as a dual-use item. Annex I sets out a list of dual-use items that require authorization for export to a destination outside of the EU.

To reiterate: the functional encryption technology as developed in the FENTEC project falls under the Regulation's definition of a 'dual-use item', and is categorized as a dual-use item under Annex I, category 5, part 2 of Regulation 428/2009 (as amended by Regulation 2015/2420).

Technology

Regulation 2015/2420 defines *'technology'* as:

> *"... specific information necessary for the "development", "production" or "use" of goods. This information takes the form of 'technical data' or 'technical assistance'.*
>
> *N.B. 1: 'Technical assistance' may take forms such as instructions, skills, training, working knowledge and consulting services and may involve the transfer of 'technical data'.*
>
> *N.B. 2: 'Technical data' may take forms such as blueprints, plans, diagrams, models, formulae, tables, engineering designs and specifications, manuals and instructions written or recorded on*

[55] Proposal for a Regulation of the European Parliament and of the Council setting up a Union regime for the control of exports, transfer, brokering, technical assistance and transit of dual-use items (recast) COM(2016) 616, 28.9.2016, 2016/0295(COD).
[56] Article 2, 1 of Regulation (EC) No 428/2009.

other media or devices such as disk, tape, read-only memories".[57]

This definition implies that 'technology' is a broad concept; including both abstract (instructions, skills, training, etc.) and concrete (blueprints, plans, models, etc.) types of information.

The Regulation sets out *General Notes to Annex I*, which establishes that:

> *"The object of the controls contained in this Annex should not be defeated by the export of any non-controlled goods (including plant) containing one or more controlled components when the controlled component or components are the principal element of the goods and can feasibly be removed or used for other purposes.*
>
> *N.B.: In judging whether the controlled component or components are to be considered the principal element, it is necessary to weigh the factors of quantity, value and technological know-how involved and other special circumstances which might establish the controlled component or components as the principal element of the goods being procured".*[58]

This expands the scope of 'technology' to also include components of systems, rather than exclusively complete systems and equipment. This prevents the exports of individual components, only to be reassembled into a complete system in the country of destination. Such a situation would completely circumvent the dual-use exports control regime.

The Regulation also sets out a *General Technology Note* (GTN), replicated from the Wassenaar controls list. This note has to be read in conjunction with section E of each dual-use item category in Annex I (for FENTEC: 5E002), and which establishes that:

> *"The export of "technology" which is "required" for the "development", "production" or "use" of goods controlled in Categories 1 to 9, is controlled according to the provisions of Categories 1 to 9".*[59]
>
> "*Technology" "required" for the "development, "production" or "use" of goods under control remains under control even when applicable to non-controlled goods".*[60]

The GTN creates a due diligence obligation to assess whether 'technology' is 'required' for the development, production, or use of controlled dual-use items. This requires a technical assessment through a factual analysis. The GTN thus only regulates 'technology' that is *'required'* for the *'development'*, *'production'* or *'use'* of goods. These concepts are defined as follows:

Required – *"... peculiarly responsible for achieving or extending the controlled performance levels, characteristics or functions ...".*[61] Here, *'peculiarly'* means *'more than usual'.*

[57] Annex I, 24 of Commission Delegated Regulation (EU) 2015/2420.
[58] Annex I, 3 of Commission Delegated Regulation (EU) 2015/2420.
[59] Annex I, 4 of Commission Delegated Regulation (EU) 2015/2420.
[60] Annex I, 4 of Commission Delegated Regulation (EU) 2015/2420.
[61] Annex I, 20 of Commission Delegated Regulation (EU) 2015/2420.

Development – *"all phases prior to serial production, such as: design, design research, design analyses, design concepts, assembly and testing of prototypes, pilot production schemes, design data, process of transforming design data into a product, configuration design, integration design, layouts,".*[62]

Production – "*all production phases, such as: construction, production… testing, quality assurance,".*[63]

Use – *"operations... maintenance… repair, overhaul and refurbishing".*[64]

> *"Controls on "technology" transfer do not apply to information "in the public domain", to "basic scientific research" or to the minimum necessary information for patent applications".*[65]

'*Basic research'* refers to experimental or theoretical research without specific practical aims or objectives.[66] This would be the case for the development of a pilot or prototype.

This exception does not apply to the FENTEC project in so far as the technology is not in the public domain and goes beyond the concept of *'basic scientific research'*.

> *"Controls do not apply to that "technology" which is the minimum necessary for the installation, operation, maintenance (checking) or repair of those goods which are not controlled or whose export has been authorized."*

Exports and exporter

Export refers to the transfer of items to a destination outside of the EU territory. This is not limited to the physical export of dual-use items, but also includes their intangible export. This is particularly relevant for intangible technologies such as the functional encryption technology developed within the FENTEC project.

Under Regulation 428/2009 an *'export'* occurs when the exporter:

i) initiates an export procedure so as to have goods, items, technology, technological assistance or know-how leave the customs-territory of the European Community,[67]

ii) re-exports non-community goods, items, technology, technological assistance or know-how to a destination outside the customs-territory of the European Community,[68]

iii) transfer technology intangibly, i.e. so-called intangible technology transfers (ITTs).[69]

The *'Intangible Technology Transfer'* (ITT) can be defined as:

"transmission of software or technology by electronic media, including by fax, telephone, electronic mail or any other electronic means to a destination outside the European Community; it includes making available in an electronic form such software and technology to legal and natural persons and

[62] Annex I, 11 of Commission Delegated Regulation (EU) 2015/2420.
[63] Annex I, 19 of Commission Delegated Regulation (EU) 2015/2420.
[64] Annex I, 25 of Commission Delegated Regulation (EU) 2015/2420.
[65] Annex I, 4 of Commission Delegated Regulation (EU) 2015/2420.
[66] Annex I, 9 of Commission Delegated Regulation (EU) 2015/2420.
[67] Article 2, 2, (i) of Regulation (EC) No 428/2009; Article 161 of Council Regulation (EEC) No 2913/92 of 12 October 1992 establishing the Community Customs Code.
[68] Article 2, 2, (ii) of Regulation (EC) No 428/2009; Article 182 of Council Regulation (EEC) No 2913/92.
[69] Article 2, 2, (iii) of Regulation (EC) No 428/2009.

partnerships outside the Community. Export also applies to oral transmission of technology when the technology is described over the telephone;".[70]

The transfer of technology is very broad and can be done in multiple ways. It is therefore advisable to only make technology available to entities located within the EU, with safeguards for possible onward transfers to third countries. A project partner might accidentally provide information to a non-EU country through various forms of communication, thereby exporting 'technology' and thus not complying with the obligations under the EU Regulations.

Whereas the Regulation specifically exemplifies ITTs through fax, telephone, mail and other transmissions, it should be remembered that that technology or technical assistance can be inadvertently provided to non-EU persons in many ways, but that particular care should be taken in situations such as when:

i) Publishing technical know-how in open-source or other journal, articles, blogs or text that can be copied or downloaded and transferred onward,
ii) Presenting technical know-how orally to international audiences or in a setting where the presentation may be filmed and transferred onward,
iii) Research collaboration with non-EU persons or persons who cannot guarantee re-use of the know-how in EU settings only,
iv) Sharing of know-how within multi-national entities where some of the offices or staff are located outside of the EU,
v) Solicitations and demonstrations, in an exploitation setting, relating to entities or persons representing non-EU entities, or whom you are unfamiliar with,
vi) Solicitations and demonstrations, in an exploitation setting, towards EU entities that cannot provide assurances against onward transfer,
vii) International and, in particular, non-EU trade fairs and exhibitions.

An **exporter** is any natural or legal person or partnership that:

i) holds a contract with a consignee in the third country and has the power for determining the sending of the item out of the customs territory of the Community, or where no contract is concluded,[71]
ii) the person with the power for determining the sending of the item outside the Community,[72] or
iii) the person who decides to transmit or make available software or technology by electronic media outside the Community.[73]

3.2.2.2 Authorizations for FENTEC

- All FENTEC partners, except NAGRAVISION SA, are established within the EU. Transfers of technology, in the context of the FENTEC project, within the EU do not require any export authorizations.

- NAGRAVISION SA is established in Switzerland. Exports to Australia, Canada, Japan, New Zealand, Norway, *Switzerland*, Liechtenstein, and the United States of America all require the *Union General Export Authorization (EUGEA) No EU001* under Annex IIa of Regulation

[70] Article 2, 2, (iii) of Regulation (EC) No 428/2009.
[71] Article 2, 3, (i) of Regulation (EC) No 428/2009.
[72] Article 2, 3, (i) of Regulation (EC) No 428/2009.
[73] Article 2, 3, (ii) of Regulation (EC) No 428/2009.

2015/2420.[74] This type of export authorization is granted by the European Union, and is subject to the conditions and requirements set out in Annex IIa. This authorization is available to all exporters of certain dual-use items and for certain countries of destination, under the conditions of Annex IIa.

- For exports to other destinations outside of the EU (destinations that do not fall under the list of Annex IIa), a national export authorization in required.[75] These authorizations are issued by the competent national authorities under conditions laid down by domestic law.
    - National General Export Authorization (NGEA) (art. 2, 11 and art. 9, 2 and 4 of Regulation (EC) No 428/2009): defined by national law or practice and granted by national competent authorities. Applies to all exporters as far as the existing EUGEA's are respected and the relevant conditions and requirements are met.
    - Individual Export Authorization (IEA) (art. 2, 8 and art. 9, 2 of Regulation (EC) No 428/2009): granted by national competent authorities to one exporter, for one end-user in a third country, covering one or more dual-use items.
    - Global Export Authorization (GEA) (art. 2, 10 and art. 9, 2 and 5 of Regulation (EC) No 428/2009): granted by national competent authorities to one exporter, for one or more end-users in one or more third countries, for a type or category of dual-use item.

Exporters must also keep detailed registers or records of their exports, containing specific information as laid down by article 20 of Regulation 428/2009.

3.3 Risks and solutions

As mentioned above, there is a relatively low risk of dual-use or misuse of FENTEC technology. Despite this low risk, it should still be acknowledged and possible mitigation strategies should be proposed. These strategies should prevent the accidental transfer of technology to a destination outside of the EU, and should consequently prevent potential dual-use and misuse thereof.

1. Create awareness about dual-use risks and mitigation strategies among partners and stakeholders.

2. Install and maintain a monitoring strategy throughout the project lifespan to ensure that the risks of dual-use are mitigated and the applications remain civil in nature. Concrete measures could be: non-disclosure agreements, limited dissemination of research findings, restricted access to the contents of the project, etc.

- New dual-use risks that emerge in the project lifespan must be identified and mitigated through appropriate mitigation measures. Concrete measures could be: limited dissemination of research findings.

- Obtain the necessary licenses and authorizations for exports to a destination outside of the EU and satisfy and accompanying obligations. With one partner from Switzerland (NAGRAVISION SA), this should be taken into account. Non-compliance with the export control regime could seriously hamper the project activities due to investigations and could even result in penalties.

- Conduct a risk-benefit assessment to weigh the benefits gained by the research and encryption technologies against the risks of their dual-use and misuse.

[74] Article 3 and article 9, 1 of Regulation (EC) No 428/2009; Annex IIa of Regulation (EC) No 428/2009.
[75] Article 3 and article 9, 2 of Regulation (EC) No 428/2009.

In any case, FENTEC technology should be kept within the EU as much as possible. If an export to a destination outside of the EU is required (f.e. to Switzerland), the accompanying legal obligations regarding dual-use should be respected (by acquiring the appropriate authorization). In this context, the consortium partners should prevent, where possible, transfers to destinations outside of the EU. They should also be careful not to accidentally transfer technology via electronic (f.e. a publication, common communication, phone conversation, etc.) or other means (f.e. a collaboration, an exhibition, a demonstration, etc.). This creates a due diligence obligation for all the partners in the chain.

As with dual-use, the misuse of FENTEC technology is a real, albeit unlikely, possibility. The risk of misuse is rather low due to the limited added value of functional encryption for criminals. The underlying reasoning is the same as for dual-use items. The identified risks and proposed mitigation strategies for dual-use items can also be applied to misuse.

3.4 Dual-use and misuse risk assessment

This section builds upon the ethical assessment carried out at the proposal stage[76] in which the risk of the Project results being misused and/or catalogued as potentially dual-use was "low" or "very low"; after further examination, the "low risk" mark is maintained as per the rationale in this section. For practical reasons, and since the analysis, conclusions, mitigation, etc. are very similar in both cases, there will not be a strict distinction between dual-use and misuse.

In any case, and although the risks are low, FENTEC project will monitor any changes and development that could affect the potential dual-use and misuse of the project results (see section 3.5). This follow up, which includes the level of compliance and an adjusted strategy when necessary, will be later presented in the reports D3.3 Legal Framework Report (due December 2019) and D3.4 Final Legal Compliance (due December 2020).

In general terms, the risk of FENTEC results being misused or transferred to military applications (e.g. dual-use) is "very-low" to "low" as per the following reasoning:

- All the research and developments in FENTEC are intended for civilian use only and aimed to be used in three specific use cases, namely: privacy-preserving digital currency, data collection and local decision making, and privacy preserving statistical analysis.
- The focus of FENTEC is Functional Encryption (FE). Compared to traditional encryption (e.g. AES, which is algorithm used by US Government[77]) it may offer more flexibility but not more security. Also, traditional encryption will always be more mature than any novel development from FENTEC. Therefore, there is no reason to assume any strong interest in the immediate results of FENTEC from the military, intelligence agencies and criminals.

The same result is obtained if the different levels in which FENTEC operates are scrutinized:

- Conceptual level: this includes core research activities and the dissemination of results, typically though scientific papers, articles, and technical publications in general (as defined in D2.2 Dissemination Plan[78]). Since there is no implementation, the utility of these results for the military and criminals is very limited. The new algorithms are not likely to offer any clear

[76] [PRO1] FENTEC Proposal (No. 780108). H2020-DS-2016-2017. FENTEC Consortium, April 2017.
[77] [NIS1] Selecting the Advanced Encryption Standard (AES): Raising the Bar for Cryptography William E. Burr. NIST, 2003, https://www.nist.gov/publications/selecting-advanced-encryption-standard-aes-raising-bar cryptography.
[78] [FEN1] D2.2 Dissemination Plan. FENTEC Consortium, June 2018.

advantage to those already known (and used, e.g. AES[79]) by the military, intelligence agencies and criminals. Therefore, the risk of dual-use and misuse of FENTEC basic research is "very low".

- Practical level: new hardware concepts to support the new developments in FE, including physical attacks. These developments have very limited value when separated from the FE algorithms, therefore at most they share the same "very low" risk.
- Implementation level: this includes the crypto API and the three prototypes. These results are more tangible than the outputs from other levels, therefore the risk is higher, albeit still low
    - Crypto API: this result is arguably the one with the higher risk since it could be used, for instance, to encrypt military communications or messages among criminals. However, there is no clear advantage when compared to traditional encryption widely used (by the military, civilian, and either lawful or unethical applications). Additionally, more details on how to control access to the API and IPR will be presented in D2.6 Exploitation Plan (due December 2019)[80]. All considered, the risk for the API is kept as "low".
    - Prototypes: more or less the same risk assessment as for the API, although possibly even lower since the implementations will be done by the Consortium and therefore there is more control on a closed final product. More details and additional protection measures (e.g. export outside the EU strategy and/or restrictions) will be included in D2.6 Exploitation Plan[81].

One additional consideration is whether the potential misuse and/or dual use of the results refers to offensive or defensive capabilities, this is respectively, to crack existing cryptography algorithms or prevent unauthorised access to private information (what has been analysed so far).

Since FENTEC focuses on developing FE, the risk of the project results being used to break existing cryptography is very low.

3.5 Monitoring and mitigation measures

Although the risk of misused and dual-use is low, FENTEC will take the appropriate measures to ensure that the project results are applied lawfully and in civilian scenarios only. The efforts to ensure that FENTEC complies with this premise can be grouped into three action-blocks: raising awareness, mitigation measures and monitoring.

3.5.1 Raising awareness - prevention

FENTEC must ensure that the members of the consortium understand the concepts of dual-use and misuse, and are aware of the implications. When applicable, this awareness needs to be extended to other stakeholders such as the Project Advisory Board (PAB), participants in Project events such as workshops, third parties interested in the crypto API and the prototypes, etc.

The main actions to raise awareness and prevent misuse/dual-use are as follows:

[79] [NIS1] Selecting the Advanced Encryption Standard (AES): Raising the Bar for Cryptogaphy William E. Burr. NIST, 2003, https://www.nist.gov/publications/selecting-advanced-encryption-standard-aes-raising-bar cryptography.
[80] [FEN2] D2.6 Exploitation Plan. FENTEC Consortium, due December 2019.
[81] [FEN2] D2.6 Exploitation Plan. FENTEC Consortium, due December 2019.

- One-time introductory training module for the Consortium. A 30-minute presentation was delivered to the Consortium by KU Leuven (FENTEC General Assembly and Technical Meeting. Helsinki, October 2018).[82] The presentation was followed by a question & answers session and some discussion to set the foundations of the risk assessment carried out in this deliverable.
- Periodical reminders, both at WP level and Project-wide. Dual-use and misuse of results are logged in the Project risk register (see section 3.5.3). Risk are recurrently discussed in WP specific conference calls and Executive Board (EB) meetings, thus reminding all partners about potential misuse and/or dual-use.
- Specific items regarding dual-use and misuse on the agenda when meeting the PAB and other stakeholders.

3.5.2 Active measures - mitigation

The efforts to prevent the dual-use and misuses of the project results will be tailored to the outputs at the different levels in which FENTEC operates (see section 3.4).

- Conceptual level: this comprises mostly scientific papers and other technical documents (articles, web entries, etc.). No specific measures needed; in general terms, these will be treated following D2.2 Dissemination Plan[83] and following the guidelines of the publisher (e.g. journal, conference, etc.).
- Practical level: developments at this level will be shared via reports and articles (e.g. hardware will not be made available to anyone, therefore same actions as for the conceptual level.
- Implementation level: this includes de crypto API and the prototypes, which are the most readily available results and therefore were the focus of the mitigation measures sits.
    - In general terms, all the information, code, the API itself, etc. made public (e.g. project website, public repositories such as GITHUB) will include a disclaimer that all the results are for civilian use only and explicitly excluding military use.
    - Concise measures, and specific for the API and the prototypes, will be defined as part of the exploitation strategy and IPR management in D2.6 Exploitation Plan[84]. These measures are likely to include limitation to the dissemination of some of the results, additional considerations for export outside the EU, restricted access to some materials and results, confidentiality and non-disclosure agreements, code obfuscation and other countermeasures against reverse engineering, etc.

When new risks are identified (see section 3.5.3) these measures will be updated accordingly, and/or new actions will be included into the risk management strategy.

3.5.3 Risk follow up – monitoring and corrective measures

In FENTEC risks are permanently monitored and managed (see D1.4 Project Handbook for the Project's risk management strategy, roles and responsibilities)[85]. Dual-use and misuse are included in the risk register and therefore recurrently discussed in Project meetings and telephone conferences.

[82] [FEN3] Presentation on Legal Requirements, including risk of dual-use and misuse of Project results. KU Leuven, October 2018, https://repository.atosresearch.eu/index.php/s/DbO1XjqrLbvdxe3.
[83] [FEN1] D2.2 Dissemination Plan. FENTEC Consortium, June 2018.
[84] [FEN2] D2.6 Exploitation Plan. FENTEC Consortium, due December 2019.
[85] [FEN4] D1.4 project Handbook. FENTEC Consortium, March 2018.

More specifically, the risk of misuse and dual-use is monitored in FENTEC as follows:

- Periodically discussed in WP and EB meetings and calls (e.g. typically at least twice a month) when project risks are addressed.
- Included in the agendas of meetings with external such as the PAB and other stakeholders.
- KU Leuven (legal expert, task leader) and the Ethical Manager (also KU Leuven) to monitor and validate the current risk management strategy. Propose amendments when needed
- KU Leuven and Ethical Manager also consulted ad hoc for specific enquiries from any Consortium partner regarding misuse or dual-use. When required, matters will be taken to Leuven Ethical Committee.
- Further assessment and/or mitigation actions to be defined when D2.6 Exploitation Plan[86] is drafted.
- If needed, adjust strategy and align actions if new risks were identified in the future, for instance when revisiting FENTEC's Dissemination and Communication activities (e.g. D2.3 - D5.5[87] and D2.8 – D2.10[88]).
- Risk assessment results, plus corrective measures when needed, to be included in D3.3 Legal Framework Report[89] and D3.4 Final Legal Compliance Report[90]. A risk-benefit analysis will also be included D3.4 Final Legal Compliance Report.

3.6 Summary of misuse and dual-use assessment and strategy

Table 1: misuse and dual-use strategy

Level	Risk Rating	Prevention	Mitigation	Monitoring
Project-Wide	Low	Ad hoc training sessions (including. external stakeholders) and periodical refreshers	Disclaimers, access control, NDA, IPR management, obfuscation, etc.	Use of risk register, discussed in meetings (e.g. EB), Ethical Manager oversees strategy and actions
Conceptual & Practical Level	Very Low			
Implementation. API & Prototypes	Low			

[86] [FEN2] D2.6 Exploitation Plan. FENTEC Consortium, due December 2019.
[87] [FEN5] D2.3 to D2.5 Annual Dissemination Report & Material. FENTEC Consortium, due December 2018, December 2019 and December 2020.
[88] [FEN6] D2.8 to D2.10 Annual Communication Activities Report. FENTEC Consortium, due December 2018, December 2019, December 2020.
[89] [FEN7] D3.3 Legal Framework Report. FENTEC Consortium, due December 2019.
[90] [FEN8] D3.4 Final Legal Compliance Report. FENTEC Consortium, due December 2020.

4 The Digital Currency Use-case

The digital currency use case employs functional encryption to create a payment system that preserves customer privacy while keeping the auditability of the system. This payment system will use digital coins of general purpose but with specialized usage. There exists, however, sector-specific legislation that applies to a payment system using a digital currency. The applicability of the Second E-money Directive (2009/110/EC), the Second Payment Services Directive (2015/2366), and the Anti-Money Laundering Directive (2015/849) will be discussed below.

4.1 The Second E-money Directive (2009/110/EC)

4.1.1 Introduction

The second attempt by the EU to regulate electronic money (e-money) resulted in the second E-money Directive (EMD2). The EMD2 aims to create a more level playing field and establishes a clearer scope; resulting in more legal certainty.[91]

4.1.2 Scope

The EMD2 applies to '*electronic money issuers*', which are recognized by the directive as; (1) credit institutions, (2) electronic money institutions, (3) post office giro institutions, (4) the European Central Bank and national central banks (when not acting in their capacity as monetary authority or other public authorities), and (5) Member States or their regional or local authorities (when acting in their capacity as public authorities).[92] The category of *electronic money institutions* can be defined as legal persons that have been granted authorisation under Title II to issue electronic money.[93] This category will make up most of the electronic money issuers and will be, together with the Member States or their local or regional authorities, the most relevant for the FENTEC use-case.

Electronic money issuers may issue e-money under the conditions of the directive. '*Electronic money*' is defined as:

> *"means electronically, including magnetically, stored monetary value as represented by a claim on the issuer which is issued on receipt of funds for the purpose of making payment transactions as defined in point 5 of Article 4 of Directive 2007/64/EC, and which is accepted by a natural or legal person other than the electronic money issuer."*[94]

This definition can be split up into *four requirements*:

1) *Electronically, including magnetically, stored monetary valu*e: this requires that the e-money funds are stored electronically and are available and accessible to the bearer, including remotely, without the intervention of a third party.[95] In the present FENTEC use-case, the

[91] N. VANDEZANDE, *Virtual Currencies: A Legal Framework*, Cambridge, Intersentia, 2018, 209-210.
[92] Article 1, 1 of Directive 2009/110/EC.
[93] Article 2, 1 of Directive 2009/110/EC.
[94] Article 2, 2 of Directive 2009/110/EC.
[95] N. VANDEZANDE, *Virtual Currencies: A Legal Framework*, Cambridge, Intersentia, 2018, 214-215.

funds are stored in the customer's electronic wallet and are available and accessible to the customer without third party intervention.

2) *Represented by a claim on the issuer:* this requirement means that the holder of the e-money is not the direct owner thereof, but rather has a claim on the issuer. This implies that the holder can demand reimbursement of the funds. In casu, the holder of the e-money can exchange the funds back to legal tender through the exchange platform.
3) *Issued on receipt of funds for making payment transactions:* the idea that e-money may only be issued on receipt of funds means that e-money is a prepaid good. Therefore, e-money issuers cannot create new e-money at will. The concept of 'payment transactions'[96] refers to a broad range of transactions which involve a transfer of monetary value between two parties.[97] In the digital currency use-case, the customer must pay funds in exchange for its equivalent in the digital currency. This constitutes an exchange and the required receipt of funds.
4) *Accepted by institutions other than their issuer:* this requirement makes a distinction between single- or limited-purpose instruments and multi-purpose instruments, which means that the e-money in question must be broadly accepted. This requirement is therefore closely related to the limited network exemption which brings e-money outside the scope of EMD2 (the limited scope exemption will be discussed in section 4.1.3).[98] For FENTEC, this requirement will be fulfilled as long as there are merchants aside from the issuer that accept the digital currency in question.

The EMD2 and its obligations apply if all four requirements are met simultaneously, and on the condition that no scope exemption applies.

4.1.3 Scope exemptions

The EMD2 contains two exemptions that will bring certain digital currencies outside the scope of the directive. These are the limited network exemption[99] and the exemption relating to providers of electronic communications networks or services[100]. For FENTEC, the limited network exemption is particularly important.

For these exemptions, the EMD2 makes reference to the First Payment Services Directive (PSD1), which was repealed by the Second Payment Services Directive (PSD2). For these references, we therefore look at the PSD2.

The EMD2 establishes that:

> "*This Directive does not apply to monetary value stored on instruments exempted as specified in Article 3 (k) of Directive 2007/64/EC.*"[101]

[96] Article 4, (5) of Directive 2015/2366 defines a 'payment transaction' as: *"an act, initiated by the payer or on his behalf or by the payee, of placing, transferring or withdrawing funds, irrespective of any underlying obligations between the payer and the payee."*
[97] N. VANDEZANDE, *Virtual Currencies: A Legal Framework*, Cambridge, Intersentia, 2018, 218-219.
[98] N. VANDEZANDE, *Virtual Currencies: A Legal Framework*, Cambridge, Intersentia, 2018, 219-220.
[99] Article 1, 4 of Directive 2009/110/EC and article 3, (k) of Directive 2015/2366.
[100] Article 1, 5 of Directive 2009/110/EC and article 3, (l) of Directive 2015/2366.
[101] Article 1, 4 of Directive 2009/110/EC.

The PSD2, in turn, says that it does not apply to:

> "*services based on specific payment instruments that can be used only in a limited way, that meet one of the following conditions:*
>
> *(i) instruments allowing the holder to acquire goods or services only in the premises of the issuer or within a limited network of service providers under direct commercial agreement with a professional issuer;*
>
> *(ii) instruments which can be used only to acquire a very limited range of goods or services;*
>
> *(iii) instruments valid only in a single Member State provided at the request of an undertaking or a public sector entity and regulated by a national or regional public authority for specific social or tax purposes to acquire specific goods or services from suppliers having a commercial agreement with the issuer."*[102]

According to this limited network exemption, the EMD2 does not apply to the FENTEC e-money in three possible cases:

- The e-money can only be used to buy goods or services in specific stores or a chain of stores that are under direct commercial agreement with the issuer.
- Only a limited range of goods or services can be acquired with the e-money. An example would be e-money that can only be used to buy childcare products or household services.
- E-money that is regulated by a public authority for specific social or tax purposes to acquire specific goods or services, such as a local government that issues e-money to acquire only baby products as social aid.

It is important to note that it is possible for a specific-purpose instrument to develop into a general-purpose instrument, which brings the e-money in question back into the scope of the directive. It is also possible that a list of merchants is provided which is continuously growing, which would also mean that the exemption does not apply.[103]

The applicability of this scope exemption does not change the qualification of the digital currency as e-money. It merely brings the e-money outside the scope of the EMD2.

4.1.4 Obligations

If the requirements for the scope are met, and the limited network exemption does not apply, the directive imposes certain obligations on the issuers of e-money. The directive distinguishes between obligations for electronic money issuers in general (Title III) and obligations for electronic money institutions specifically (Title II). Depending on the further specification of the digital currency use-case and the national implementations of the EMD2, these obligations may be relevant for the FENTEC use-case. As the applicability of the EMD2 is not yet clear, a broad overview of the obligations will be given.

4.1.4.1 Electronic money institutions

Electronic money institutions must abide by several rules in addition to the common rules applicable to all electronic money issuers.

[102] Article 3, (k) of Directive 2015/2366.
[103] Recital 5 of Directive 2009/110/EC; Recital 13 and 14 of Directive 2015/2366.

1) *General prudential rules*. These rules make reference to the PSD1. They deal with the authorisation and registration of the electronic money institutions, as well as their relation with and supervision by the competent authorities.[104] They also include procedural rules on mergers and takeovers.[105]
2) *Initial capital and own funds.* Electronic money institutions must have an initial capital of at least EUR 350 000.[106] They must also hold own funds equal to at least 2% of the average outstanding electronic money, or not less than EUR 350 000, whichever is higher.[107]
3) *Additional activities*. An electronic money institution may also conduct additional activities, such as the provision of payment services. They may, however, not take deposits or other repayable funds.[108]
4) *Safeguarding requirements.* Electronic money institutions must safeguard the funds that they have received in exchange for e-money. The specific methods of safeguarding are determined by the Member States.[109]
5) *Optional exemptions.* Member States may, under certain conditions, waive the entire or partial application of specific rules, namely article 3, 4, 5, and 7 of the EMD2.[110]

4.1.4.2 Electronic money issuers

Electronic money issuers, thus including electronic money institutions, are subject to a set of general rules.

1) *Issuance and redeemability.* E-money must, at all times, be issued at par value on the receipt of funds. The monetary value of the e-money must also be redeemable at any moment and at par value. Redeeming e-money may only be subject to a fee if it is stated in the contract and only in the specified cases.[111]
2) *Prohibition of interest.* Granting interest or any other benefit related to the length of time during which an e-money holder holds e-money is prohibited.[112]

4.2 The Second Payment Services Directive (2015/2366)

4.2.1 Introduction

The PSD2 establishes rules on the transparency of conditions and information requirements for payment services and creates rights and obligations for payment service providers (PSP) and users. It aims to further harmonize the payments market in the EU and create more legal certainty in order to support the growth of the Union economy and to allow consumers, merchants and companies can fully benefit from the internal market.[113]

[104] Article 3, 1 of Directive 2009/110/EC.
[105] Article 3, 3 of Directive 2009/110/EC.
[106] Article 4 of Directive 2009/110/EC.
[107] Article 5, 1 of Directive 2009/110/EC.
[108] Article 6 of Directive 2009/110/EC.
[109] Article 7 of Directive 2009/110/EC.
[110] Article 9 of Directive 2009/110/EC.
[111] Article 11 of Directive 2009/110/EC.
[112] Article 12 of Directive 2009/110/EC.
[113] Recital 4 and 5 of Directive (EU) 2015/2366.

4.2.2 Scope

4.2.2.1 Personal scope

The PSD2 applies to and distinguishes between several categories of '*payment service providers*': (1) credit institutions, (2) electronic money institutions, (3) post office giro institutions, (4) payment institutions, (5) the European Central Bank and national central banks (when not acting in their capacity as monetary authority or other public authorities), and (6) Member States or their regional or local authorities (when not acting in their capacity as public authorities).[114]

The concept of a '*payment transaction*' is crucial to both the personal and material scope of the PSD2. It is defined as:

> "*an act, initiated by the payer or on his behalf or by the payee, of placing, transferring or withdrawing funds, irrespective of any underlying obligations between the payer and the payee.*"[115]

This definition refers to a broad range of possible transactions which involve a transfer of monetary value between two parties and would include a transaction of e-money.

For FENTEC, the most relevant category will be the electronic money institutions. PSD2 establishes that it regulates the execution of payment transactions where the funds are e-money, and that is does not regulate the issuance of e-money itself. For this reason, payment institutions should not be allowed to issue e-money.[116] As described above in section 4.1.2, the FENTEC digital currency constitutes e-money, which means that its issuer cannot be a payment institution.

4.2.2.2 Material scope

The PSD2 applies to '*payment services*' provided by payment service providers. These services are laid down in an exhaustive list in Annex I:

"1. Services enabling cash to be placed on a payment account as well as all the operations required for operating a payment account.

2. Services enabling cash withdrawals from a payment account as well as all the operations required for operating a payment account.

3. Execution of payment transactions, including transfers of funds on a payment account with the user's payment service provider or with another payment service provider:

(a) execution of direct debits, including one-off direct debits;

(b) execution of payment transactions through a payment card or a similar device;

(c) execution of credit transfers, including standing orders.

4. Execution of payment transactions where the funds are covered by a credit line for a payment service user:

(a) execution of direct debits, including one-off direct debits;

(b) execution of payment transactions through a payment card or a similar device;

(c) execution of credit transfers, including standing orders.

5. Issuing of payment instruments and/or acquiring of payment transactions.

6. Money remittance.

[114] Article 1, 1 of Directive (EU) 2015/2366.
[115] Article 4, (5) of Directive (EU) 2015/2366.
[116] Recital 25 of Directive (EU) 2015/2366.

7. *Payment initiation services.*
8. *Account information services."*[117]

The PSD2 will apply to the relevant payment service provider in so far as their activities in the use-case constitute any of the abovementioned payment services. Only payment service providers that provide payment services as part of their main or regular occupation or business activity should fall under the PSD2.[118]

4.2.2.3 Geographic scope

In terms of applicable obligations, the PSD2 also makes a distinction based on where the payment services are provided:

1. The directive applies to payment services provided in the EU.[119]
2. Titles III and IV apply to payment transactions in a Member State currency where both the payer's and payee's PSPs are, or the sole PSP is, located within the EU.[120]
3. Titles III and IV (with exceptions) apply to payment transactions in a non-Member State currency where both the payer's and payee's PSPs are, or the sole PSP is, located within the EU, for those parts of the payment transaction carried out within the EU.[121]
4. Titles III and IV (with exceptions) apply to payment transactions in all currencies where only one PSP is located within the EU, for those parts of the payment transaction carried out within the EU.[122]

4.2.3 Scope exemptions

The limited network exemption is described in section 4.1.3. It applies in the same way to payments services as it does to e-money. Therefore, the same reasoning may be applied meaning that the FENTEC use-case may fall outside of the scope of the PSD2.

In the situation that the limited network exemption applies, and the total value of payment transactions over the preceding 12 months exceeds EUR 1 million, the payment service provider must notify the competent authorities of a description of the payment service offered. The competent authority will then make a decision whether or not the payment service falls under the limited scope exemption.[123]

4.2.4 Obligations

4.2.4.1 Transparency of conditions and information requirements

These obligations apply to single payment transactions and payment transactions covered by framework contracts. Low-value payment instruments and e-money may not be subject to certain obligations in so far as they satisfy the conditions laid down by article 42.

[117] Annex I of Directive (EU) 2015/2366.
[118] Recital 24 of Directive (EU) 2015/2366.
[119] Article 2, 1 of Directive (EU) 2015/2366.
[120] Article 2, 2 of Directive (EU) 2015/2366.
[121] Article 2, 3 of Directive (EU) 2015/2366.
[122] Article 2, 4 of Directive (EU) 2015/2366.
[123] Article 37, 2 of Directive (EU) 2015/2366.

First, in case of single payment transactions, there is prior general information that has to be made available to the payer. This information must be given in an easily accessible manner, in easily understandable words, in a clear and comprehensible form, and in an official language of the Member State where the service is offered.[124] This prior general information includes: a specification of the information to be provided by the user which is necessary to initiate and execute the payment service, the maximum execution time of the service, and the charges that have to be paid by the user.[125]

Secondly, after the receipt of the payment order, the payer's payment service provider must provide the payer with certain information. This information includes: a reference for identification of the payment transaction, the amount of the payment transaction, the charges that have to be paid by the payer, and the date of receipt.[126]

Lastly, after the execution of the payment transaction, the payee's payment service provider must provide the payee with certain information. This information includes: a reference for identification of the payment transaction, the amount of the payment transaction, the charges that have to be paid by the payee, and the credit value date.[127]

For payment transactions covered by a framework contract, there are similar information obligations. These obligations are laid down in articles 51 to 58 and deal with prior general information, information before the execution of the payment transaction, and information after the execution of the payment transaction.

In situations where charges are requested or reductions are offered, prior information should be given. Charges must only be paid if their full amount was made known prior to the initiation of the payment transactions.[128]

4.2.4.2 Rights and obligations of payment service users and providers

Here, the PSD2 makes a difference between consumers and non-consumer. If the payment service user is not a consumer, an agreement may be concluded for the non-application of certain rights and obligations.[129] Low-value payment instruments and e-money may also not be subject to certain obligations in so far as they satisfy the conditions laid down by article 63.

The applicability of the specific rights and obligations relating to the payment service user and provider depend on further specification of the use case, particularly the capacity of the payment service provider and its specific activities. These rules relate to consent, authentication, surcharging, liability, receipt and refusal of payment orders, etc. There are, however, some general obligations and observations that are of particular importance.

First, payment service providers must establish a framework with appropriate mitigation measures and control mechanisms to manage the operational and security risks relating to the payment services provided by them. In this context, they must maintain effective incident management procedures (e.g. detection and classification of major operational and security incidents).[130] In the case of such a major

[124] Article 44 of Directive (EU) 2015/2366.
[125] Article 45 of Directive (EU) 2015/2366.
[126] Article 48 of Directive (EU) 2015/2366.
[127] Article 49 of Directive (EU) 2015/2366.
[128] Article 60 of Directive (EU) 2015/2366.
[129] Article 61 of Directive (EU) 2015/2366.
[130] Article 95 of Directive (EU) 2015/2366.

operational or security incident, the payment service provider must notify the competent authorities. The payment service users must also be informed where the incident may have an impact on them.[131]

Secondly, the obligation for payment service providers is the application of strong customer authentication. They must employ adequate security measures to protect the confidentiality and integrity of personalised security credentials.[132]

A last important observation is the applicability of the GDPR to the processing of personal data for the purposes of the PSD2. The processing of personal data by payment systems and payment service providers shall be allowed when necessary to safeguard the prevention, investigation and detection of payment fraud.[133] Payment service providers can only access, process, and retain personal data with explicit consent of the user, and only when necessary for the provision of the payment services.[134]

4.3 The Anti-Money Laundering Directive (2015/849)

4.3.1 Introduction

The Anti-Money Laundering Directive (AMLD) aims to prevent the use of the EU financial system for money laundering and terrorist financing.[135] The idea is to combat serious forms of crime that are associated with money laundering and terrorist financing. The AMLD aims for minimum harmonization, which allows Member States to adopt or retain, within the limits of EU law, stricter provisions than what is provided by the AMLD.[136]

4.3.2 Scope

4.3.2.1 Material scope

The AMLD establishes that money laundering and terrorist financing are strictly prohibited.[137]

'*Money laundering*' is a broad concept that is made up of four layers. It is defined in article 1, 3 of the AMLD as:

(1) the conversion or transfer of property, *knowing that* such property is derived from criminal activity or from an act of participation in such activity, for the purpose 1. of concealing or disguising the illicit origin of the property or 2. of assisting any person who is involved in the commission of such activity to evade the legal consequences of his action.
(2) the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of property, *knowing that* such property is derived from criminal activity or from an act of participation in such activity;
(3) the acquisition, possession or use of property, *knowing*, at the time of receipt, that such property was derived from criminal activity or from an act of participation in such activity;

[131] Article 96, 1 of Directive (EU) 2015/2366.
[132] Article 97 of Directive (EU) 2015/2366.
[133] Article 94 of Directive (EU) 2015/2366.
[134] Article 94, 2 of Directive (EU) 2015/2366.
[135] Article 1 of Directive (EU) 2015/849.
[136] Article 5 of Directive (EU) 2015/849.
[137] Article 1, 2 of Directive (EU) 2015/849.

(4) participation in, association to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the actions mentioned in the foregoing points.

The definition of money laundering refers to '*property*', which is defined as:

> *"assets of any kind, whether corporeal or incorporeal, movable or immovable, tangible or intangible, and legal documents or instruments in any form including electronic or digital, evidencing title to or an interest in such assets."*[138]

This definition of property is also very broad and includes electronic money such as in the FENTEC use-case.

4.3.2.2 Personal scope

The directive applies to several obliged entities. Some of these entities are relevant to the digital currency use-case. These include: (1) credit institutions, (2) auditors that provide aid, assistance or advice on tax matters as a professional activity, (3) exchange services between virtual currencies and fiat currencies, and (4) custodian wallet providers.[139]

In order to determine the applicability of the AMLD to the FENTEC use-case, certain definitions must be given and analysed.

A '*virtual currency*' is defined as:

> "*a digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically."*[140]

The FENTEC e-money meets all requirements of this definition, except in the case of a public authority issuing the e-money for social purposes. It is not necessarily attached to a legally established currency, and it does not possess a legal status of currency or money because it cannot be qualified as legal tender.[141] It is, however, accepted by natural or legal persons as a means of exchange. It can also be transferred and traded electronically, as well as stored electronically on an e-wallet.

The qualification as a virtual currency means that the exchange platform will also qualify as a provider of exchange services between virtual currencies and fiat currencies. The AMLD will therefore apply to the exchange platform in FENTEC.

A *'custodian wallet provider*' is defined as:

> "*an entity that provides services to safeguard private cryptographic keys on behalf of its customers, to hold, store and transfer virtual currencies."*[142]

[138] Article 3, (3) of Directive (EU) 2015/849.
[139] Article 2, (a), (g), and (h) of Directive (EU) 2015/849.
[140] Article 3, (18) of Directive (EU) 2015/849.
[141] N. VANDEZANDE, *Virtual Currencies: A Legal Framework*, Cambridge, Intersentia, 2018, 216.
[142] Article 3, (19) of Directive (EU) 2015/849.

The FENTEC e-money will be functionally encrypted to ensure privacy and auditability. The AMLD will be applicable to wallet providers that holds customers' keys in order to hold, store and transfer the virtual currency. The applicability will therefore depend on the wallet provider in question, as the definition seems to exclude wallet providers not holding customers' keys.

4.3.3 Obligations

4.3.3.1 Customer due diligence

The AMLD contains ***three levels*** of customer due diligence obligations with varying measures. A risk-based approach is used to determine the necessary level of due diligence and the extent of the measures undertaken.

1. **Standard customer due diligence**

The obliged entity must take measures to identify the customer and verify the customer's identity on the basis of documents, data or information form a reliable and independent source.[143] The entity must also assess and obtain information on the purpose and intended nature of the customers' business relationship.[144] This includes ongoing monitoring of that business relationship so that the transactions are consistent with the entity's knowledge of the customer, the business, and risk profile.[145]

Obliged entities must apply customer due diligence measures in specified circumstances. These include, but are not limited to: the establishment of a business relationship, the carrying out of certain occasional transactions, there exists a suspicion of money laundering or terrorist financing, and when there are doubts about the veracity or adequacy of customer identification data.[146] The initial verification of identity of the customer must take place before the business relationship is established or transaction is carried out.[147]

With regards to e-money, Member States may allow obliged entities to not apply certain customer due diligence measures. This is the case when the risk is low and specific risk-mitigating conditions are met.[148] These derogations do not apply in all cases, such as when the e-money is redeemed or withdrawn in cash for an amount that exceeds EUR 50.[149]

2. **Enhanced customer due diligence**

The enhanced customer due diligence measures apply when there is a heightened risk. Situations of higher risk are determined by articles 18a to 24, or by the obliged entity or Member State based on the factors of potentially higher-risk set out in Annex III.

In certain cases of heightened risk, obliged entities must gather more information on the background and purpose of transactions.[150]

[143] Article 13, 1, (a) of Directive (EU) 2015/849.
[144] Article 13, 1, (c) of Directive (EU) 2015/849.
[145] Article 13, 1, (d) of Directive (EU) 2015/849.
[146] Article 11 of Directive (EU) 2015/849.
[147] Article 14 of Directive (EU) 2015/849.
[148] Article 12, 1 of Directive (EU) 2015/849.
[149] Article 12, 2 of Directive (EU) 2015/849.
[150] Article 18a, 1, (a) of Directive (EU) 2015/849.

3. **Simplified customer due diligence**

In cases where there is a lower risk, simplified customer due diligence measures may apply. Whether or not these measures apply is determined by the Member States.[151] In these cases, it is not necessary to verify the identity of the customer. However, sufficient monitoring is still required in order to detect unusual or suspicious transactions.[152] The obliged entities and Member States should take the factors of potentially lower risk situations into account, as laid down in Annex II.[153]

4.3.3.2 Reporting obligations

Obliged entities are required to inform the Financial Intelligence Unit (FIU) on their own initiative when they know, suspect or have reasonable grounds to suspect that funds are the proceeds of criminal activity or are related to terrorist financing. They must also provide necessary information when requested by the FIU.[154] Such a disclosure of information in good faith shall not constitute a breach of any restriction imposed by contract or by legislative, regulatory, or administrative provisions, and shall also not result in liability.[155] The obliged entities shall also not tip-off the customer or other third parties about the fact that information is disclosed.[156]

4.3.3.3 Data protection and record-retention

Obliged entities must retain documents and information for the purpose of preventing, detecting and investigating possible money laundering or terrorist financing.[157] Furthermore, the processing of personal data under the AMLD is subject to the GDPR.[158] This is particularly important for the customer due diligence obligations, which involve the processing of personal data. The AMLD also establishes that the processing of personal data in the context of the AMLD is considered a matter of public interest.[159]

4.3.3.4 Supervision

The AMLD also provides for a specific registration obligation for providers of virtual currency exchange services and custodian wallet providers.[160]

4.3.3.5 Sanctions

The AMLD also establishes that Member States must ensure that obliged entities can be held liable and sanctioned for breaches of the national implementation of the AMLD. These can include administrative and criminal sanctions, to be decided by the Member States.[161]

[151] Article 15, 1 of Directive (EU) 2015/849.
[152] Article 15, 3 of Directive (EU) 2015/849.
[153] Article 16 of Directive (EU) 2015/849.
[154] Article 33 of Directive (EU) 2015/849.
[155] Article 37 of Directive (EU) 2015/849.
[156] Article 39 of Directive (EU) 2015/849.
[157] Article 40 of Directive (EU) 2015/849.
[158] Article 41 of Directive (EU) 2015/849.
[159] Article 43 of Directive (EU) 2015/849.
[160] Article 47 of Directive (EU) 2015/849.
[161] Article 58 of Directive (EU) 2015/849.

5 The Web Analytics Use-case

5.1 General

This use-case addresses the privacy-preserving computation of data-analytics, with a focus on statistics over large usage data. Data on access patterns of web services can be used for various purposes such as the improvement of the performance of the service, market research, or commercial purposes. The solutions proposed by FENTEC allows the benefits of web analytics to be applied in more sensitive situations, opening up new markets. Users will have assurance their data is only used for statistical analysis, and not for services they do not want to receive or other harmful purposes. Placing control over user data in the hands of the users by preserving their privacy could restore confidence in web analytics.[162]

Awless is an open-source command line interface that allows the creation, update and deletion of resources on Amazon Web Services. Awless is used by AWS developers, which are mostly code and system developers. Analysis of access pattern data concerning Amazon Web Services can be used to optimize the services deployed on AWS. FE technology could be incorporated into the instances deployed to provide developers with information about the users of their systems.[163]

Sector-specific legislation will be discussed below to the extent that they might be relevant.

5.2 The Electronic Commerce Directive (2000/31/EC)

5.2.1 Objective and scope

This Directive aims to ensure the free movement of information society services between Member States, thereby contributing to the proper functioning of the internal market.

It applies to '*information society services*'[164], which are services that are:

(1) normally provided for remuneration
(2) at a distance
(3) by electronic means
(4) at the individual request of a recipient of services

The directive will apply to this use-case if the Awless service meets these criteria, which it does if the service is requested by the individual user of the service (e.g. developers).

5.2.2 Obligations

The obligations of this directive relate to: (1) information requirements, (2) commercial communications, (3) electronic contracts, and (4) the liability of intermediary service providers.

These obligations are not necessarily relevant for Awless, but the qualification as an information society service does have implications for the application of the ePrivacy Directive.

[162] D 3.1 Technical Requirement Analysis Report, FENTEC Consortium, May 2018, 18-19.
[163] D 3.1 Technical Requirement Analysis Report, FENTEC Consortium, May 2018, 19-21.
[164] Article 2, (a) of Directive 2000/31/EC.

5.3 The ePrivacy Directive (2002/58/EC)

5.3.1 Objective and scope

The ePrivacy Directive exists alongside the GDPR as *lex specialis*, and thus particularises and complements the GDPR.[165] It aims to ensure an equivalent level of protection of rights such as privacy and confidentiality with regards to the processing of personal data in the electronic communications sector.[166]

It applies to the processing of personal data with regards to the provision of publicly available electronic communications services in public communications networks in the EU.[167]

An '*electronic communications service*' is:

> "*a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, but exclude services providing, or exercising editorial control over, content transmitted using electronic communications networks and services; it does not include information society services, as defined in Article 1 of Directive 98/34/EC, which do not consist wholly or mainly in the conveyance of signals on electronic communications networks.*"[168]

If the information society service consists wholly or mainly in the conveyance of signals on electronic communications networks (e.g. the internet), then the ePrivacy Directive applies. This is the case if the service does not provide or exercise editorial control over the content that is transmitted.

In the context of the ePrivacy Directive, consent has the same meaning as under the GDPR. This means that the consent requirements of the GDPR apply. Consent must therefore be freely given, be specific and informed, and constitute an affirmative action.[169]

5.3.2 Obligations

A first obligation relates to the security of processing data. The provider of a publicly available electronic communications service must safeguard the security of its services by taking appropriate technical and organizational measures. These measures will vary based on the risks involved.[170] Specific minimum requirements are laid down, such as the protection of personal data against unauthorized or unlawful storage, processing, access or disclosure.[171] This is where encryption schemes, such as FE, can play an important role.

Another important obligation under the directive relates to the storing of information, or the access to information already stored, in the terminal equipment of users. These activities are only allowed if consent has been obtained from the user. Information must also be given with regards to the purposes of processing. The obligation to obtain consent does not apply in the following cases:

[165] Article 1, 2 of Directive 2002/58/EC.
[166] Article 1, 1 of Directive 2002/58/EC.
[167] Article 3 of Directive 2002/58/EC.
[168] Article 2 of Directive 2002/58/EC; Article 2, (c) of Directive 2002/21/EC.
[169] Recital 17 of Directive 2002/58.
[170] Article 4, 1 of Directive 2002/58/EC.
[171] Article 4, 1a of Directive 2002/58.

(1) the technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network; or
(2) as strictly necessary in order for the provider of an information society service explicitly requested by the user to provide the service.[172] Strictly necessary means that it must be essential to fulfil the request of the user.

This obligation is especially important to the use of cookies, which are placed in the terminal equipment of the user.

Lastly, the directive also lays down rules for traffic and location data, which are respectively defined as:

> "*any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof*"[173]
>
> *"any data processed in an electronic communications network or by an electronic communications service, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service."*[174]

Traffic data on users processed and stored by service providers must be erased or made anonymous when it is no longer necessary for the purpose of the transmission of a communication.[175] Prior explicit consent of the user is required for the processing of traffic data for the purpose of marketing electronic communications services.[176] This requires the service provider to inform the user, prior to obtaining consent, of the types of traffic of traffic data and the duration of processing.[177]

Location data other than traffic data on users may only be processed when they are made anonymous or with the consent of the user. For this type of data, the user must also be informed prior to obtaining consent. This information must include the type of data which will be processed, the purpose and duration of processing, and whether the data will be transmitted to a third party.[178]

5.4 The ePrivacy Regulation

In the coming years, the new ePrivacy Regulation will replace the current ePrivacy Directive of 2002. It is, however, not clear when the proposal of the ePrivacy Regulation will be formally adopted. As with any proposal, it is still subject to change. It is therefore necessary to monitor its further development in order to apply it to the Awless use-case.

5.4.1 Objective, scope, and obligations

The changing digital landscape and the emergence of new types of services and applications necessitates a revision of the existing rules on ePrivacy in the EU. New types of services that are functionally similar or nearly identical to legacy services are now included in the scope of ePrivacy.

[172] Article 5, 3 of Directive 2002/58.
[173] Article 2, (b) of Directive 2002/58.
[174] Article 2, (c) of Directive 2002/58.
[175] Article 6, 1 of Directive 2002/58.
[176] Article 6, 3 of Directive 2002/58.
[177] Article 6, 4 of Directive 2002/58.
[178] Article 9, 1 of Directive 2002/58.

According to the latest proposed changes to the Regulation, the rules on ePrivacy will apply to the processing of electronic communications content and of electronic communications metadata carried out in connection with the provision and the use of electronic communication services. They will also apply to end-user' terminal equipment information.[179]

The scope of application has been broadened by adapting the definition of 'electronic communications service' and by introducing new concepts, such as the concept of 'interpersonal communications service'.

'*Electronic communications service*' is defined as:

> "*a service normally provided for remuneration via electronic communications networks, which encompasses 'internet access service' as defined in Article 2 (2) of Regulation (EU) 2015/2120; and/or 'interpersonal communications service'; and/or services consisting wholly or mainly in the conveyance of signals such as transmission services used for the provision of machine-to-machine services and for broadcasting, but excludes services providing, or exercising editorial control over, content transmitted using electronic communications networks and services."*[180]

As there is no explicit mention of information society services anymore, it is not clear whether or not they will fall under the scope of the ePrivacy Regulation. There is, however, still mention of 'services consisting wholly or mainly in the conveyance of signals'.

A first obligation relates to electronic communications data (both content data and metadata). These data shall only be processed if:

(1) it is necessary to achieve the transmission of the communication, for the duration necessary for that purpose; or
(2) it is necessary to maintain or restore the security of electronic communications networks and services, to detect technical faults, errors, security risks, and/or attacks in the transmission of electronic communications.[181]

Additionally, and without prejudice to the above, providers of electronic communications networks and services shall only process metadata if:

(1) it is necessary for the purposes of network management or optimization, provided that the purpose(s) could not be fulfilled by processing anonymous information.
(2) the end-user has given consent, provided that the purpose(s) could not be fulfilled by processing anonymous information.

Another important obligation relates to the protection of end-user' terminal equipment information. The use of processing and storage capabilities of terminal equipment and the collection of information from terminal equipment is prohibited, unless:

[179] Article 2 of the Proposal for a Regulation on Privacy and Electronic Communications, Examination of the Presidency text, 20 September 2018, 2017/0003(COD).
[180] Article 4, 1, (b) of the Proposal for a Regulation on Privacy and Electronic Communications, Examination of the Presidency text, 20 September 2018, 2017/0003(COD); Article 2, (4) of Directive establishing the European Electronic Communications Code.
[181] Article 6, 1 of the Proposal for a Regulation on Privacy and Electronic Communications, Examination of the Presidency text, 20 September 2018, 2017/0003(COD).

(a) it is necessary for the sole purpose of carrying out the transmission of an electronic communication over an electronic communications network; or
(b) the end-user has given consent; or
(c) it is necessary for providing an information society service requested by the end-user; or
(d) it is necessary for *audience measuring*, provided that such measurement is carried out by the provider of the information society service requested by the end-user or by a third party on behalf of the provider, and provided that the conditions of Article 28 of the GDPR are met.[182]

This last element is relevant for cookies used for audience measuring. The new proposal also establishes that consent is not required for non-privacy intrusive cookies that are used for the improvement of the internet experience.

Over the last year, the obligations of the Regulation have been amended several times. These examples illustrate the possibility of application of the Regulation and its possible contents. As said before, no definite claims can be made regarding this applicability.

[182] Article 8, 1 of the Proposal for a Regulation on Privacy and Electronic Communications, Examination of the Presidency text, 20 September 2018, 2017/0003(COD).

6 The Internet of Things Use-case

6.1 General

Over the past years, the EC has taken actions to accelerate the take-up of IoT and to transform society into a digitized and interconnected environment. As part of the efforts to reach the goals of the Digital Single Market strategy, the EC published the European Commission staff working document on "Advancing the Internet of Things in Europe"[183]. This document sets out the IoT vision of the EU and is centered around three key points: (1) a thriving IoT ecosystem, (2) a human-centered IoT approach, and (3) a single market for IoT.

In order for IoT technologies to be trusted, accepted, and used, they must first comply with legal obligations as found in the GDPR and relevant sector-specific legislation. Privacy, data protection, and security are important issues that can heavily influence acceptance and adoption of IoT technologies. For this reason, effective security solutions such as strong encryption are crucial.

The 2017 cybersecurity package, as mentioned in section 2.2.3, also acknowledges the rapidly changing digital environment. It stresses the importance of the concept of security by design, especially for IoT technologies. The package also contains a proposal for an EU cybersecurity certification framework[184]. This framework will introduce common security standards for IoT devices on the EU level. A more uniform certification framework can lower the fragmentation of national security standards and certification schemes, and in turn increase the trust of users.

The following sections will look at the sector-specific instruments applicable to video surveillance and smart meters, and whether or not specific requirements can be identified. Since there are no comprehensive EU-wide rules on video surveillance, we analyze Belgian camera law as an example of national legislation.

6.2 Video surveillance

This video surveillance use-case makes use of video cameras (IoT edge device) with motion detection. The video stream is encrypted end-to-end, while the motion vectors in the stream are functionally encrypted. This functional encryption scheme enables local decision-making at the gateway level while preserving privacy and security. These local decisions allow for better balancing of the load of the network; saving bandwidth and preserving storage.

Video surveillance, or closed-circuit television (CCTV), generate large amounts of data which can be used to identify individuals and keep records of their activities. Its use has far-reaching implications for the right to privacy and data protection of individuals. With the GDPR becoming applicable on the 25th of May, organizations have less freedom in their data collection and processing practices. The GDPR,

[183] Commission staff working document: Advancing the Internet of Things in Europe, 19 April 2016, SWD(2016) 110 final.

[184] Proposal for a Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act"), 13 September 2017, COM(2017) 477 final.

however, is not the only legal instrument applicable to CCTV. Considering the implications CCTV, national law may also regulate the use of cameras for surveillance. As an example, the next section will give a brief overview of the new Belgian Camera Act.

6.2.1 The Belgian Camera Act

6.2.1.1 Subject matter and scope

The revised Belgian Camera Act, applicable from the 25th of May 2018, regulates the use of surveillance cameras in specified and defined areas.

The scope of application is limited to surveillance cameras, which are cameras that are intended to be used to survey and guard certain areas.[185] These surveillance cameras must have the purpose of: (1) preventing, capturing, or detecting criminal offences against persons or property, (2) preventing, capturing, or detecting hindrance, (3) monitoring compliance with municipal regulations, or (4) upholding public order. The law does not apply to cameras installed and used by the police, or in the workplace for certain purposes.[186]

The applicability of the law and the accompanying legal obligations also depend on the location of the surveillance camera. A distinction is made between surveillance cameras placed in (1) non-enclosed areas (e.g. a public road), (2) enclosed areas accessible to the public (e.g. a shop), and (3) enclosed areas not accessible to the public (e.g. company offices).

6.2.1.2 Obligations

The applicable legal obligations may vary depending on the location of the surveillance camera. There are, however, certain key obligations:

1) Record keeping: the controller must keep a register of the processing activities of the surveillance cameras. This obligation exists on top of the record-keeping obligation under article 30 of the GDPR.
2) Notification to the police: the controller must notify the police of its decision to install surveillance cameras.
3) Use of pictograms: the controller must make use of pictograms to publicly disclose the use of surveillance cameras.

The law also regulates the right of access to the images. Generally, only the controller and the person recorded on tape (data subject) are allowed to have access to the images.[187]

Lastly, surveillance cameras may not capture images aimed at providing information on the philosophical, religious, political, and syndical beliefs, the ethnic or racial origin, the sex life, or health of a person.[188] These categories of information are very similar to the special categories of sensitive personal data found in article 9 of the GDPR. Capturing images aimed at providing biometric information is not prohibited. This is because surveillance cameras are often used to physically identify persons and gather evidence.

[185] Article 2, 4 of the Act of 21 March 2007 regulating the installation and use of surveillance cameras.
[186] Article 3 of the Act of 21 March 2007 regulating the installation and use of surveillance cameras.
[187] Article 9 and 12 of the Act of 21 March 2007 regulating the installation and use of surveillance cameras.
[188] Article 10 of the Act of 21 March 2007 regulating the installation and use of surveillance cameras.

This example illustrates that national camera laws may specify the type of cameras, the specific location, and under what condition they are allowed. For the video surveillance use-case it is important to identify the applicable national law. In a controller environment where no personal data is processed, this will not pose many problems.

The Information Commissioner's Office (ICO), which is the UK national data protection authority, has also revised its code of practice for surveillance cameras and personal information.

6.3 Smart meter

The EU has placed a large focus on the development of smart grids as they would allow for better and more efficient energy management and reduce emissions in the EU. It is therefore not surprising that the rollout of smart meters is crucial to this EU vision. There are several EU instruments that regulate the energy sector which are relevant for smart meters.

6.3.1 The Electricity Directive (2009/72/EC), Natural Gas Directive (2009/73/EC), and Energy Efficiency Directive (2012/27/EU)

The EU encourages Member States to take actions for the modernization of distribution networks; for example, through the introduction of smart grids.[189] Member States shall also promote energy efficiency by recommending that electricity and natural gas undertakings introduce intelligent metering systems or smart grids.[190]

The aim of the EU is to equip 80% of consumers with intelligent metering systems by the year 2020. Such a rollout would occur when the results of the accompanying cost-benefit analysis are positive.[191]

This aim is reiterated multiple times in the Energy Efficiency Directive.[192] Depending on the results of the economic assessment, smart meters will soon be wide-spread across the EU. In order to facilitate the rollout, the EC has made recommendations to Member States regarding (1) data protection and security considerations, (2) the methodology for the economic assessment, and (3) minimum functional requirements for smart meters for electricity.[193] These minimum requirements include secure data communications and fraud prevention.

The Energy Efficiency Directive defines the concepts of *'smart metering system'* and '*intelligent metering system'* as:

> "*an electronic system that can measure energy consumption, providing more information than a conventional meter, and can transmit and receive data using a form of electronic communication*".[194]

When the abovementioned rollout occurs, Member States are obliged to take certain actions that protect and benefit the final customer. Two of these obligations determine that Member States shall ensure:

[189] Recital 27 of Directive 2009/72/EC.
[190] Article 3, 11 of Directive 2009/72/EC; Article 3, 8 of Directive 2009/73/EC.
[191] Article 2 of Annex I of Directive 2009/72/EC; Article 2 of Annex I of Directive 2009/73/EC.
[192] Recital 27 and 31 of Directive 2012/27/EU.
[193] Commission Recommendation 2012/148/EU on preparations for the roll-out of smart metering systems.
[194] Article 2, (28) of Directive 2012/27/EU.

> "*that the objectives of energy efficiency and benefits for final customers are fully taken into account when establishing the minimum functionalities of the meters and the obligations imposed on market participants*"[195]

> "*the security of the smart meters and data communication, and the privacy of final customers, in compliance with relevant Union data protection and privacy legislation*"[196]

These requirements will gain substance in the national implementations of the Directive and could differ greatly between Member States. Furthermore, the rules and requirements of this Directive aim for minimum harmonization. Member States are allowed to maintain or impose more stringent rules and requirements.[197] For the use of smart meters, it is therefore advised to consider the requirements laid down by national Member State laws.

6.3.2 Proposal for a recast of the Electricity Directive

The proposal for a recast of the Electricity Directive[198] contains several articles relating to different aspects of smart meters.

Member States must, where there is a positive economic assessment or a systematic rollout of smart meters, ensure that they are implemented in line with several principles. These principles reflect minimum functionalities relating to security, privacy and data protection, and technical aspects.[199]

Examples of relevant minimum functionalities are:

> "*the security of the smart metering systems and data communication is ensured in compliance with relevant Union security legislation having due regard of the best available techniques for ensuring the highest level of cybersecurity protection"*[200]

> "*the privacy and data protection of final customers is ensured in compliance with relevant Union data protection and privacy legislation"*[201]

These provisions refer to other EU legislation, and must be further specified by the Member States on a national level.

Even where there is a negative economic assessment, or no systematic rollout, Member States must ensure that final customers can request a smart meter that meets these minimum functionalities, or a set of minimum functionalities as defined by the Member State.[202]

---

[195] Article 9, 2, (a) of Directive 2012/27/EU.
[196] Article 9, 2, (b) of Directive 2012/27/EU.
[197] Article 1, 2 of Directive 2012/27/EU.
[198] Proposal for a Directive of the European Parliament and of the Council on common rules for the internal market in electricity (recast), 23 February 2017, COM(2016) 864 final/2.
[199] Article 20 of the Proposal for a Directive of the European Parliament and of the Council on common rules for the internal market in electricity (recast).
[200] Article 20, (b) of the Proposal for a Directive of the European Parliament and of the Council on common rules for the internal market in electricity (recast).
[201] Article 20, (c) of the Proposal for a Directive of the European Parliament and of the Council on common rules for the internal market in electricity (recast).
[202] Article 21 of the Proposal for a Directive of the European Parliament and of the Council on common rules for the internal market in electricity (recast).

The proposal also deals with data management and exchange of data. It creates an obligation for Member States to determine which eligible parties may have access to data with the explicit consent of the final customer.[203] In order to ensure compliance with the Directive, Member States must authorize and certify the parties which are managing data.[204] It is therefore up to the Member States to organize data management.

6.3.3 The Network and Information Systems Directive (2016/1148)

6.3.3.1 Introduction

The NIS Directive aims to increase the overall level of cybersecurity in the EU by developing a common approach and coordinating Member States' actions. The obligations contained in the directive relate to both Member States and the private sector. Section 2.2.2 provides more background information on the NIS Directive.

6.3.3.2 Scope

The NIS Directive is also relevant for the use of smart meters in the FENTEC project. A smart meter falls under the definition of a '*network and information system*' through its qualification as a:

> "*device or group of interconnected or related devices, one or more of which, pursuant to a program, perform automatic processing of digital data.*"[205]

The obligations of the NIS Directive apply to '*operators of essential services*', which is defined as:

> "*a public or private entity of a type referred to in Annex II, which meets the criteria laid down in Article 5 (2).*"[206]

Annex II mentions energy suppliers and distribution system operators, which are also, depending on the Member State, the operators of smart meters. These entities qualify as operators of essential services if they meet the criteria laid down in article 5, (2):

1. *An entity provides a service which is essential for the maintenance of critical societal and/or economic activities*. This condition is easily met by energy suppliers and distribution system operators. Without their services, critical societal and economic activities would not be possible. The functioning of society would be seriously hampered in case of loss of the energy supply.
2. *The provision of that service depends on network and information systems*: This is also true for energy suppliers and distribution system operators. These entities make use of network and information systems to organize, conduct, and monitor their services.
3. *An incident would have significant disruptive effects on the provision of that service*: The meaning of '*significant disruptive effect*' is determined by the Member States, taking into account certain factors as laid down by article 6, 1 of the NIS Directive. The existence of such a significant disruptive effect depends heavily on factors relating to the specific entity in

[203] Article 23, 1 of the Proposal for a Directive of the European Parliament and of the Council on common rules for the internal market in electricity (recast).
[204] Article 23, 3 of the Proposal for a Directive of the European Parliament and of the Council on common rules for the internal market in electricity (recast).
[205] Article 4, (1), (b) of Directive (EU) 2016/1148.
[206] Article 4, (4) of Directive (EU) 2016/1148.

question, such as; the number of users relying on the service, their market share, the geographic area potentially affected, the degree and impact of the incident, etc.[207]

In the end, it is up to the Member States to identify the operators of essential services with an establishment on their territory. If the energy supplier or distribution system operator is identified as an operator of an essential service, and they also operate smart meters, then the obligations of the NIS Directive will apply to the security of these smart meters.

6.3.3.3 Obligations

Operators of essential services must take appropriate and proportionate technical and organizational measures to manage risks to the security of their network and information systems.[208] They must also take appropriate measures to prevent and minimize the impact of incidents affecting the security of the network and information systems.[209] The specific substance of these measures is determined on a Member State level and will therefore differ between Member States.

These operators must also notify the competent authority or the CSIRT of incidents having a significant impact on the continuity of the provided services. Such a notification must include information that enables the competent authority or CSIRT to determine any cross-border impact of the incident.[210] To determine the significance of the impact, specific factors must be taken into account.[211]

The competent authorities can also require operators of essential services to provide:

(a) Information necessary to assess the security of their NIS (e.g. security policies).
(b) Evidence of the effective implementation of such security policies (e.g. results of security audits).[212]

If the entity that operates the smart meters is identified as an operator of essential services, they must take these obligations into account. As the directive is vague in its specific requirements, it is important to consult national legislation.

6.3.4 Smart grid DPIA template

The Data Protection Impact Assessment Template for Smart Grid and Smart Metering systems[213], drawn up by Expert Group 2 of the Smart Grid Task Force, is also relevant in this field. This voluntary DPIA Template is addressed to smart grid operators, including smart meter operators, and aims to support these operators with GDPR compliance. Although this template is non-compulsory, it could contribute to a common application and approach to the GDPR by smart grid operators. The use of the DPIA from the very beginning is also beneficial to the implementation of the data protection by design principle, which is especially important in the IoT environment. Even though no personal data will be processed in the IoT use-cases, it could still serve as a guiding instrument for activities after the research phase.

[207] Article 6, 1 of Directive (EU) 2016/1148.
[208] Article 14, 1 of Directive (EU) 2016/1148.
[209] Article 14, 2 of Directive (EU) 2016/1148.
[210] Article 14, 3 of Directive (EU) 2016/1148.
[211] Article 14, 4 of Directive (EU) 2016/1148.
[212] Article 15, 2 of Directive (EU) 2016/1148.
[213] Data Protection Impact Assessment Template for Smart Grid and Smart Metering systems of 13 September 2018, https://ec.europa.eu/energy/sites/ener/files/documents/dpia_for_publication_2018.pdf, last accessed 29 November 2018.

7 Conclusion

In this deliverable, relevant and applicable ethical and legal framework and principles for the FENTEC project were laid down.

First, relevant instruments, such as the GDPR and Convention 108, were discussed and analysed. Relevant expert opinions and high-level guidance documents were discussed at relevant points, such as the OECD Guidelines for cryptography policy, ENISA's Opinion Paper on encryption and UNESCO's report on Human rights and encryption. Even though no personal data will be used for FENTEC research, they are taken into account to facilitate compliance of the product once it's used in a real-life setting.

Then, the issue of dual use and misuse of encryption was tackled. Dual use refers to use of functional encryption by the military, whereas misuse means functional encryption technologies being used by criminals or terrorists. The risk of dual use or misuse in FENTEC is quite low; nevertheless, the project coordinator has provided certain measures against them.

The next three sections present the FENTEC use cases: digital currency scenario, anonymous AWLESS data collection and smart camera – internet of things scenario. Different rules and legislations apply to these use cases. Since legislation is quite fragmented on European and national levels, it is a challenge to delineate between different fields of application, especially in the digital currency scenario. Moreover, ePrivacy rules are changing, leading to uncertainty about the exactness of the new regime, let alone about its entering into force. Regarding the Internet of Things use case, the use of security cameras or CCTV is left to member states to regulate. We have described the Belgian camera law as an example of member state level regulation. Moreover, we have analyzed relevant European cybersecurity legislation and energy legislation for comparison in order to feed into further legal research.

Based on our analysis of applicable legal instruments and the progress of use cases, we will draft a table of specific requirements to be met by FENTEC technologies and use case implementations. Since law is abstract and high-level by its very nature, its specific obligations for developers cannot be fully formulated until the scenarios are fully and finally formulated. Moreover, as FENTEC research includes no personal data, we are focusing on requirements to be met by the final product and its inclusion in an operational environment. At this stage, applicability of certain legal instruments, such as the payment services directive, cannot be fully determined, therefore their obligations will be mapped in the next deliverable (D3.3), due M24. In this way, developers can receive meaningful guidance on legal and ethical compliance.

Functional encryption technologies contribute to privacy and security of personal data, especially in an online, connected environment. Despite no personal data being used in FENTEC research, once the technologies are marketable and used in a real-life scenario, there will most likely be individuals – data subjects. To this end, technical partners will be continued to be provided with legal and ethical guidelines. Twice a year, a general consortium meeting is convened, at which major legal and ethical issues will be discussed. Moreover, the ethics manager is participating in the regular executive telcos in order to monitor current legal and ethical challenges and project compliance. If necessary, additional legal and ethics training will be provided, as has already been done for the GDPR in April 2018.

The work begun in this task will be continued in task T3.3, resulting in reports D.3.3.1 and D3.3.2. These reports will feed from this deliverable, resulting in a requirement monitoring table and final

compliance report. The next two legal reports, due in M24 and M36, will build upon this deliverable in order to guide the consortium toward legal and ethical compliance.

In Task T3.3, the legal management and final compliance of the project with relevant data protection, privacy and security legislation will be assessed and reviewed. The implementation of the requirements identified in Task 3.3 in the project and its use cases will be monitored continuously for the duration of the project. Ongoing guidance, feedback and assistance will be provided to the technical partners, thus ensuring that legal and ethical norms are considered during development to fully adhere to the principles of security- and privacy-by-design. To ensure an efficient and real-time requirement monitoring a "requirements monitoring table" will be created summarizing the legal and principles, the category of requirements and prioritization, the actions suggested from legal and ethical perspective and the actions taken by the project partners.

Next thereto legal experts will further monitor and acknowledge legal and policy developments at the national and European level, such as the implementation of new legislation, the issuance of relevant and binding case law, and the adoption of opinions and advices of legal and data protection authorities. New requirements may be extracted and suggestions for their implementation, for mitigation techniques and best practices may be made. Through interdisciplinary cooperation the actual impact of new requirements on the technical developments in the project and the feasibility to incorporate will be evaluated case-by-case. The ultimate goal of this task is to ensure that technologies developed throughout the project are not only compliant with applicable legislative norms, but also support the implementation of legal rights and duties in practice. In particular, this will be done for the three identified use cases and the specific contexts in which the technology shall be implemented. This valuable legal research on the use of innovative encryption techniques from a privacy, ethical and legal point of view is intended to be valorised by means of publications and dissemination.

Annexes

Annex I: FENTEC GDPR do's and don'ts

FENTEC GDPR do's and don'ts

DO: **Be aware** that the GDPR (General Data Protection Regulation, 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) is entering into force on May 25 2018 and that:

- It applies to FENTEC and to you as a researcher
- Compliance with GDPR is a strong selling point for any FENTEC products / applications /…
- In order to efficiently achieve compliance, privacy and data protection have to be taken into account already at the beginning of the project = privacy by design.

DON'T: **process personal data in the FENTEC research activities**. The ethics table in our GA indicates that no personal data will be processed.

- For ATOS it is specified that the digital currency system (testing) will use **mock-up data**
- For Kudelski Security it is specified that the testing of IoT use-cases will rely on **fabricated data**
- For Wallix it is specified that an **anonymous data** collection will be created relying on functional encryption in the Amazon awless client: "Using the core results of the FENTEC project, Wallix will use Functional Encryption to encrypt the user data directly on the user device. As only encrypted data will be collected without knowledge of the decryption keys, Wallix will be able to compute statistics over multiple users but will not be able to retrieve or decrypt the data of any single user."

DO: One especially important principle to take into account in all FENTEC developments is **privacy/data protection by default** (Art. 25). This principle entails that: "appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed" are implemented, "That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons."

DON'T: **Forget about** the person who is the final end-user of any FENTEC product, or product which incorporates FENTEC developments. Somewhere, there is always going to be a **data subject**. Depending on the purpose of the data processing, the legal ground which allows the data processing and several other – case specific or sector specific – parameters, this person will have strong rights: to information, to access, to be forgotten, to review decisions,…

DO: **Take care of your documentation**. Under GDPR data controllers and data processors will have to keep a lot of documentation. You can make their life easier and your products better sellable when your developments are well documented: mapping of data flows, mapping of technological solutions to legal and ethical requirements,…

References for basic guidelines on GDPR:

There are several guidance documents available on achieving GDPR compliance. Below are a few that focus (inter alia) specifically on **data protection by design and data security requirements**:

- Deloitte: privacy by design and by default: LINK
- Privacy trust: LINK
- Hunton & Williams law firm's GDPR guide – data protection by design on p. 21, and data breach obligations on pp. 24-25
- Norton Rose Fulbright's GDPR checklist: data protection by design on p. 7 and data breach requirements on p. 23

Recently the European Commission has also published more **general guidance documents** on achieving GDPR compliance:

- European Commission's self-assessment tool (rolled out on Jan 29 2018)

Data protection impact assessment (DPIA) is required for certain processing activities. Since FENTEC research activities will not involve processing personal data, it is not likely to be a project requirement; however, as its role is to manage risks to privacy, the right to data protection and other fundamental human rights, it will be relevant once use case scenarios are defined, and the final FENTEC solution is implemented in practice. There is no definitive DPIA methodology; it is up to the data controller to choose the most relevant one. A few guidance documents are already available:

- Working Party 29, an advisory body to the Commission, has released guidelines on DPIA – Annex I provides links to already existing DPIA's within EU framework
- DPIA's can incorporate ISO standards for PIA's (privacy impact assessments) as part of the risk management process (especially ISO/IEC 29134:2017). However, compared to PIA's, DPIA's focus on broader risks to fundamental rights.

Annex II: Privacy by design methodology

Who takes an action?

- The development team during the FE development process
- The use-case owners when testing the FE
- FENTEC adopters and their subcontractors when implementing FENTEC products

What is the objective?

- Complying with the GDPR
- In particular, complying with the data quality principles that are laid down in Article 5 of the GDPR: lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality; accountability
- Enabling data subjects (users of products and services, in which the FENTEC product is implemented) to exercise their rights regarding data protection (for example, the right to erasure)

When should it be done?

- When the FE is implemented

- FENTEC adopters – throughout the use of the FENTEC products

How should it be done? Taking into account:

- The state of the art
- The cost of implementation
- The nature, scope, context and purposes of processing
- The risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing

What action should be taken?

- Technical and organisational measures
- Implementation of safeguards into the processing
- Effective measures – translating requirements into the practice

First step: carrying out a data protection impact assessment (DPIA):

1. Establish (future) data flows, types of data and data subjects (users)
2. Set out internal and external risks, such as non-compliance with data quality principles, e.g. data minimisation principle, hacker attack, poor access controls, misuse of data by an internal risk factor (insider threat)
3. Map solutions and mitigation actions to risks

The DPIA should be followed by implementation of solutions and mitigation actions into the products and services using FE.

The DPIA should be continually re-assessed and updated if necessary. While an update may not be necessary during the research phase, when FENTEC adopters carry out a DPIA in a post-project phase, they must re-assess it and update it at least when there is a change of the risk represented by processing operations. Accordingly, adjustments may need to be made in the development or implementation of the FE in order to address these new risks.