FENTEC

D3.3 Legal Framework Report

Document Identification			
Status	Final	**Due Date**	31/12/2019
Version	1.0	**Submission Date**	30/12/2019

Related WP	WP3	**Document Reference**	D3.3
Related Deliverable(s)	D3.1, D3.2, D7.1	**Dissemination Level (*)**	PU
Lead Participant	KU Leuven-CITIP	**Lead Author**	Danaja Fabcic, Wim Vandevelde (KU Leuven)
Contributors	Prof. dr. Anton Vedder, Laurens Naudts, Danaja Fabcic, Wim Vandevelde (KU Leuven)	**Reviewers**	Marco Lewandowsky (FUAS)

Keywords:
Legal requirements, legislation, regulation, encryption, security of personal data, data protection, privacy, GDPR, e-money, payment services, anti-money laundering, video surveillance, eCommerce, ePrivacy

Document Information

List of Contributors	
Name	Partner
Anton Vedder	KU Leuven
Laurens Naudts	KU Leuven
Wim Vandevelde	KU Leuven
Danaja Fabcic	KU Leuven

Document History			
Version	Date	Change editors	Changes
0.1	30/04/2019	KU Leuven	ToC
0.2	13/06/2019	KU Leuven	Detailed ToC with section outline
0.3	08/08/2019	KU Leuven	Input in general sections
0.4	06/12/2019	KU Leuven	Input in use-case sections
0.5	12/12/2019	KU Leuven	Final changes before review
0.6	18/12/2019	KU Leuven	Final changes after review
1.0	30/12/2019	ATOS	Final version for submitting

Quality Control		
Role	Who (Partner short name)	Approval Date
Deliverable leader	Wim Vandevelde (KU Leuven)	20/12/2019
Technical Manager	Michel Abdalla (ENS)	30/12/2019
Quality Manager	Diego Esteban (ATOS)	30/12/2019
Project Coordinator	Francisco Gala (ATOS)	30/12/2019

Table of Contents

List of Tables

List of Figures

List of Acronyms

Abbreviation / acronym	Description
AML	Anti-money laundering
BEUC	Bureau Européen des Unions de Consommateurs
CFT	Combating the financing of terrorism
CJEU	Court of Justice of the European Union
DPA	Data protection authority
DPIA	Data protection impact assessment
DPO	Data protection officer
EBA	European Banking Authority
ECCS	European cybersecurity certification scheme
EDPB	European Data Protection Board
EMD2/EMD II	E-money Directive II
ENISA	European Union Agency for Cybersecurity
ESA	European supervisory authority
FAFT	Financial Action Task Force
FIU	Financial Intelligence Unit
GDPR	General Data Protection Regulation
IAM	Identity and access management
ISS	Information society service
IT	Information technology
KYC	Know your client
MEP	Member of the European Parliament
MiFID2/MiFID II	Markets in Financial Instruments Directive II
MiFIR	Markets in Financial Instruments Regulation
MLD	Anti-Money Laundering Directive
MS	Member State(s)
PbD	Privacy by Design
PEP	Politically exposed person
PSD2/PSD II	Payment Services Directive II
PSP	Payment service provider

Executive Summary

This deliverable represents the outcomes of the work carried out under T3.3 (WP3) – 'Review of legal management and compliance of the project'.

Firstly, it builds further upon D3.2, which identified the applicable legal frameworks in the context of the FENTEC research and specific use-cases. This deliverable identifies and analyses the legal requirements derived from the applicable legal frameworks (the GDPR, the Cybersecurity Act, the second E-money Directive, the second Payment Services Directive, the Anti-Money Laundering Directive, the Belgian Camera Act, the eCommerce Directive, and the ePrivacy framework).

Secondly, this deliverable will serve as the basis for D3.4, which provides a final legal validation and review of the data management in the project and compliance with regulatory norms.

1 Introduction

1.1 Purpose of the document

Deliverable 3.3 'Legal Framework Report' reports on the outcomes of T3.3 'Review of legal management and compliance of the project'.

This report builds further upon D3.2, which identified and analysed the applicable legal frameworks in the context of FENTEC research and specific use-cases. The purpose of this deliverable is to further analyse these frameworks, in order to identify applicable legal requirements and provide detailed implementation guidelines for the research and each of the use-cases. A 'requirements monitoring table' has been developed which summarizes the legal principles, the category of requirements, their prioritization, and provides for actions to be taken by the project partners. It reflects the ongoing developments in both the project as well as in the European policy and legal framework.

This deliverable will also serve as the basis for D3.4, which will monitor legal and policy developments in order to identify possible new requirements and suggestions for their implementation, for example in the context of the ePrivacy framework and certification schemes under the Cybersecurity Act. It will also analyse the applicability of the Machinery Directive (2006/42/EC), the Open Data Directive (2019/1024), and the liability and accountability frameworks. These subjects will be discussed in D3.4 due to their primary relevance in a post-research setting.

1.2 Structure of the document

This document will be structured as follows:

- Section 2 addresses the overarching features of the FENTEC development process stemming from privacy, data protection and cybersecurity legal frameworks, identified in the previous legal deliverable D3.2. More specifically, we describe the updates in the legal framework, focusing on the General Data Protection Regulation (the process of adopting the new ePrivacy framework is described in the relevant use-case section). Then, we focus on specific obligations contained in the GDPR, relevant for functional encryption scenarios, and certification schemes under the Cybersecurity Act.
- Section 3 focuses on the digital currency scenario. We describe legal obligations contained in financial regulation (Second Payment Services Directive, Anti-Money Laundering Directives, Second e-Money Directive to a smaller extent), as well as their interaction with the regime in the GDPR.
- Section 4 details the legal requirements for the video surveillance scenario. These requirements are derived from the GDPR and, as an example of applicable national legislation, the Belgian Camera Act.
- Section 5 analyses the GDPR, eCommerce Directive, and ePrivacy framework in order to identify the relevant legal requirements for the web analytics use-case.
- Finally, legal obligations are extracted into a table of requirements, containing, inter alia, the summary of legal principles, category of requirements and their prioritization. The annex also provides implementation guidelines.

2 Privacy, data protection and cybersecurity: overarching features

2.1 Updates in the data protection legal framework

2.1.1 General Data Protection Regulation (GDPR)

On May 25 2018 the General Data Protection Regulation (GDPR)[1] entered into force. The GDPR applies to the ***processing of personal data*** wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system. ***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*** is defined as 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.

The GDPR's applicability was examined in-depth in the deliverable D3.2 Legal requirement analysis report, submitted in M12 of the project. Naturally, during the research and creation of the deliverable, the challenges in legal practice have brought forward new questions, resulting in new case-law. The legal academia has likewise responded to the effects of the new regulation in practice. Moreover, there is now new expert guidance by the newly established European Data Protection Board, formerly the Article 29 Data Protection Working Party. We analyse some of those documents in this section.

2.1.2 GDPR national implementation and relevant case-law

While the GDPR is a regulation, meaning it applies directly without need for national transposition, it left some questions open for Member States (MS) to regulate. For example, while art. 83 lays out the general rules for imposing fines, such as overarching principles and the maximum amount of fines, the procedure, competences and legislating other penalties is left up to the Member States. Similarly, article 85 requires Member States to reconcile the right to the protection of personal data with the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression, and to do so *by law* (emphasis added).

Since the research in FENTEC does not involve personal data, it means that neither the GDPR nor its national implementations are applicable. In fact, the scope of application of national law will largely depend on where and by whom the final product will be used.

Comprehensive overviews of GDPR implementations are available at:

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) OJ L 119, 4.5.2016, p. 1–88.

- Free University Brussels's Privacy Hub: https://lsts.research.vub.be/en/specifying-the-gdpr/
- Bird & Bird Law firm: https://www.twobirds.com/en/in-focus/general-data-protection-regulation/gdpr-tracker

Secondly, there has been new case law by the European Court of Justice, based on preliminary rulings on GDPR-questions.

The notion of joint controllership

Art. 4(7) of the GDPR defines *data controller* as "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". Art. 26 specifies that if two or more controllers jointly determine the purposes and means of processing, they are considered *joint controllers*. In this case, they are required to determine their respective responsibilities for compliance with the obligations under the GDPR in a transparent manner. More specifically, they must clarify the exercise of the rights of the data subject and their respective duties to provide the information to the data subject.

Since the provision is quite vague and it is not always clear whether two parties are joint controllers, or if one of them is carrying out processing on behalf of the other, and should therefore be considered a *data processor* (art. 4(8)). Two cases of the Court of Justice of the European Union (CJEU) shed some light on the issue.

1. **Case C-210/16, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH[2]**

Wirtschaftsakademie Schleswig-Holstein was running a fan page hosted on Facebook, where they were offering educational services. However, neither Wirtschaftsakademie nor Facebook at that time informed visitors of the fan page that information of them was collected via cookies. When the local data protection authority (DPA) started proceedings against the Wirtschaftsakademie, the latter's defence was that it was not a data controller since it did not have factual or legal influence on the purposes and means of processing. The case made it to court, and following several appeals, eventually to the Federal Administrative Court, which stayed the proceedings and asked the CJEU six questions. Two are relevant for the notion of joint controllership:

1) Can there be responsibility for an entity which is not a controller?

2) Art. 17(2) of Directive 95/46 provides an obligation for the controller to choose a processor carefully. Since this obligation is only for controllers, can it be said that in case an entity is not a controller the entity doesn't have this obligation?

However, this was based on a flawed premise, according to the Advocate General. The data controller plays a fundamental role under the legal framework as the responsible entity for data protection compliance. The notion has to be interpreted on a factual rather than a formal analysis and given a broad interpretation, in order to ensure the effective and complete protection of data subjects. Such an analysis means taking into account who in reality determines the "purposes and means" of the data processing.

[2] For a more in-depth analysis of the case, see Schroers, J. (2018), The Wirtschaftsakademie case: Joint Controllership, available at https://www.law.kuleuven.be/citip/blog/the-wirtschaftsakademie-case-joint-controllership/.

Since Facebook's motivation for enabling users to create fan pages is to improve its advertising system, whereas Wirtschaftsakademie's role was to provide the target demographic for such goals, Facebook as well as Wirtschaftsakademie should be considered joints controllers.

Nevertheless, as the Advocate General observes in points 75 and 76 of his Opinion, that the existence of joint responsibility does not necessarily imply equal responsibility of the various operators involved in the processing of personal data. On the contrary, those operators may be involved at different stages of that processing of personal data and to different degrees, so that the level of responsibility of each of them must be assessed with regard to all the relevant circumstances of the particular case.

2. Fashion ID Case C-40/17, Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV[3]

In the Fashion ID case, this online retailer, embedded on its website the Facebook 'Like' button. When a visitor consults the website of Fashion ID, that visitor's personal data are transmitted to Facebook Ireland as a result of that website including that button. Transmission occurs without that visitor being aware of it regardless of whether or not he or she is a member of the social network Facebook or has clicked on the Facebook 'Like' button.

The Verbraucherzentrale NRW, a consumer protection group, brought proceedings against the retailer, to stop its practices. However, the retailer argued that it was not a data controller, since it has no influence either over the data transmitted by the visitor's browser from its website or over whether and, where applicable, how Facebook Ireland uses those data.

Six questions were asked, and they can be summarized as:

1. Is Fashion ID a controller, simply by the fact that it has embedded a plugin on its website that enables the transmission of personal data to a third party?
2. Should Fashion ID or the plugin-provider obtain consent from visitors and inform them about the processing?

According to the court's analysis, Fashion ID appears to have embedded on its website the Facebook 'Like' button, made available to website operators by Facebook Ireland, while fully aware of the fact that it serves as a tool for the collection and disclosure, by transmission, of the personal data of visitors to that website, regardless of whether or not the visitors are members of the social network Facebook. The court points out that by embedding that social plugin on its website, Fashion ID exerts a decisive influence over the collection and transmission of the personal data of visitors to that website to the provider of that plugin, Facebook Ireland, which would not have occurred without that plugin. The reason why Fashion ID (implicitly) consented to the collection and disclosure by transmission of the personal data of visitors to its website by embedding such a plugin on that website is in order to benefit from the commercial advantage. This means those processing operations are performed in the economic interests of both Fashion ID and Facebook Ireland. It therefore appears that both parties determine the purposes of the operations involving the collection and disclosure of personal data, *jointly*.

In other words:

> "The fact that Fashion ID does not have *access to the data* collected and transmitted to Facebook did not change CJEU's conclusion on joint controllership. Similarly, Fashion ID's argument that it is not a controller because it has *no influence* over the data transmitted and how it is used

[3] For an analysis of the case, see Christofi, A. (2019) The Fashion ID judgment: broad definition of (joint) controllership solidified, available at https://www.law.kuleuven.be/citip/blog/the-fashion-id-judgment-broad-definition-of-joint-controllership-solidified/.

by Facebook was dismissed. What appeared crucial for the Court was that Fashion ID, motivated from a commercial interest, allowed Facebook to collect and use data that the latter would otherwise have not got."[4]

Decision by German DPA, relevant to encryption

In the federal state of Sachsen-Anhalt (Germany), a fine of EUR 3700 was issued due to sending of an unencrypted mail with health data to a wrong recipient. However, we were not able to find any more details about the decision.[5]

2.1.3 New guidance by the European Data Protection Board (EDPB)

The European Data Protection Board was established by the GDPR to replace the previous Article 29 Working Party. It functions as an advisory body to the European Commission on privacy and data protection related matters. It is composed of representatives of national data protection authorities, which grants its otherwise non-binding guidelines a great weight in terms of expertise.

1. Guidelines on video surveillance[6]

Considering the intrusive nature of video surveillance technologies and the significant impact on the lives and behavior of individuals, the EDPB has recently issued guidelines on the processing of personal data through video devices. While useful for certain specific purposes, the wide-spread use of video surveillance devices gives rise to the risk of creating a chilling effect on the behavior of individuals. Additionally, the large amount of data collection and the processing of personal data for unexpected purposes has considerable implications for the rights and freedoms of individuals, including the right to privacy and data protection. Today, processing activities also increasingly include analysis through the use of smart technologies and algorithms, which in turn produces even more data. The EDPB guidelines describe how the GDPR applies in the context of personal data processing through video devices and explains how to comply with data protection principles in different situations.

2. Opinion 5/2019 on the interplay between the GDPR and ePrivacy regime[7]

In this Opinion, dated 12 March 2019 and requested by the Belgian Supervisory Authority, the EDPB tackled the question of potential overlaps between the GDPR and the ePrivacy Directive (Directive 2002/58/EC on privacy and electronic communications). The latter applies more specifically to the *processing of personal data in the electronic communications sector*, and may act as a *lex specialis* to GDPR's *lex generalis*. The key takeaways from this report are:

- Processing may fall within the scope of both laws at the same time;[8]

[4] Ibid.
[5] GDPR Enforcement Tracker, http://www.enforcementtracker.com/.
[6] European Data Protection Board, Guidelines 3/2019 on processing of personal data through video devices, adopted on 10 July 2019.
[7] European Data Protection Board, Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities.
[8] See also the case by the CJEU: Case C-673/17, Bundesverband der Verbraucherzentralen und Verbraucherverbände — Verbraucherzentrale Bundesverband eV v Planet49 GmbH.

- For example: cookies that are placed on the user's device and may be used to identify them, together with other identifiers, such as RFID tags or IP address;
- Controllers which fall under the combined scope of both laws, may not rely on any of the six legal grounds in the GDPR, but must instead look to the ePrivacy regime, for example obtain consent before accessing information, stored on the user's device;
- Under art. 95 of the GDPR, a single personal data breach notification either under this article or the ePrivacy regime to relevant authorities, is sufficient.

3. Guidelines 4/2019 on Article 25 - data protection by design and by default[9]

The current version of the new PbD guidelines was adopted by the EDPB on 13 November 2019, just before the due date of this deliverable. The core obligation of art. 25 of the GDPR is the effective implementation of the data protection principles and data subjects' rights and freedoms by design and by default. The guidelines explain the notions of "the state of the art", clarify the balancing test contained in art. 25(1), give some guidance on the implementation of data protection principles, and also specifically mention encryption several times. The key ideas of this report are:

- Encryption or hashing are a form of pseudonymisation (not anonymization, implicitly)
- Examples of safeguarding measures envisioned in art. 25: enabling data subjects to intervene in the processing, providing automatic and repeated information about what personal data is being stored, or having a retention reminder in a data repository. Another may be implementation of a malware detection system on a computer network or storage system in addition to training employees about phishing and basic "cyber hygiene".
- The notion of risk in art. 25 is identical to the one in art. 35 – referring to the Guidelines on Data Protection Impact Assessment[10]
- Pseudonymisation and separate key storage are a measure contributing to the implementation of the data minimisation principle (para. 71) and to the integrity and confidentiality principle (para. 80)
- Certification under art. 42 of the GDPR is an element to demonstrate compliance

2.2 Types of data used in FENTEC project

GDPR applies to processing of personal data. As explained above, in order to qualify data as personal, they must meet four criteria:

1. Any information
2. Relating to
3. An identified/identifiable
4. Natural person

Inversely, if data have been fully anonymized and depersonalized, the GDPR does not apply when they are being processed. Anonymized data is described in Recital 26 as information which does not relate

[9] Available at: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201904_dataprotection_by_design_and_by_default.pdf.

[10] Article 29 Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is 'likely to result in a high risk' for the purposes of Regulation 2016/679, WP 248.

to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. Such data might be used for statistical or research purposes but it will not fall under the GDPR regime. Nevertheless, other legislation may apply, for example national legal frameworks on accessing archived data or on freedom of information, or the processing of data may fall under the wide-reaching legal regime of art. 8 of the European Convention on Human Rights, i.e. the right to privacy.[11]

There is no prescribed standard of anonymisation in the EU legislation, nor a specifically prescribed technique. The state of anonymisation must be as final and as irreversible as erasure,[12] which might be difficult given that computational power has increased and re-identification is possible despite previous anonymisation. Potential identifiability depends on specific circumstances analysis – what are the costs of re-identification, which means does the controller have at its disposal and how reasonably likely it is to employ them. If there is no potential linkability between data in a dataset or in different datasets, then the data is considered anonymised and GDPR does not apply any more.[13]

However, the threshold for data being considered anonymized is quite high.

Data, used in FENTEC use-cases

Partners, involved in the FENTEC project will test its new functional encryption technologies in three use-cases. All three use-cases will specifically avoid the use of personal data for FENTEC validation. As already explained in D3.2, non-personal data will suffice for validation purposes.

In the use-case "Privacy-preserving and auditable Digital Currency" (in this document: "Digital Currency Scenario") a digital-based currency will be provided as a one-to-one counterpart to physical, money centrally-distributed or issued as convenient as debit and credit cards, without its privacy issues but still allowing some opportunities of taxability or auditability by governments or its taxes agencies. The digital currency system (testing) will use **mock-up data.**

In the second use-case, "Data Collection and Local Decision Making" (in this document: "Smart Camera Scenario"), a secure key distribution method that facilitates the controlled distribution of data among a vast number of IoT devices, as required for device management and orchestration purposes, will be prototyped. The testing of IoT use-cases will rely on **fabricated data.**

Lastly, the use-case "Privacy-Preserving Statistical Analysis" (in this document: "Web Analytics scenario") addresses the privacy-preserving computation of data analytics. Specifically, it focuses on the computation of statistics over large usage data. Statistical functions include mean, standard deviation, number, sum and min/max, to name a few examples. An **anonymous data** collection will be created relying on functional encryption in the 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."

[11] Some more examples are given by the Article 29 Working Party in its Opinion 04/2007 on the Concept of Personal data, Section IV.
[12] Article 29 Working Party, Opinion 05/2014 on Anonymisation Techniques, p. 6.
[13] Article 29 Working Party, Opinion 05/2014 on Anonymisation Techniques, p. 8-9.

2.3 Legal requirements from the GDPR

Despite the absence of personal data in FENTEC research, the design of the final product strives to be legally compliant. This means addressing GDPR requirements early on in the development project in accordance with the **privacy by design principle**. This principle has been formally implemented in the GDPR, and is discussed in this section, together with other requirements, important for the FENTEC research setting.

2.3.1 Data quality principles (art. 5(1))

Personal data must be processed **lawfully, fairly and in a transparent manner** in relation to the data subject.[14] Lawfulness refers to processing having appropriate legal grounds, as set out in article 6, such as consent, or if processing is necessary in order to perform a contract, comply with a legal obligation, protect the vital interests of the data subject or of another natural person, perform a task in the public interest or for legitimate interests pursued by the controller, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject.

Purpose limitation means that data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.[15] This principle establishes 'the boundaries within which personal data collected for a given purpose may be processed and may be put to further use.'[16] It consists of two building blocks:

- data is collected for specified, explicit and legitimate purposes,
- further processing of collected data must not be done in a way incompatible with those purposes (article 5(1)b).

Specific purpose means that the purpose must be 'sufficiently defined to enable the implementation of any necessary data protection safeguards, and to delimit the scope of the processing operation'. An explicit purpose is one that is 'sufficiently unambiguous and clearly expressed'. Legitimate purpose requires legal grounds for data processing, which go beyond the scope of privacy rules and refer to the legal system as a whole.[17]

Data must be collected in a way that is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed according to the **data minimisation** principle.[18]

Under the **accuracy** principle, data must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.[19]

According to **storage limitation principle**, data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. It may be stored for longer periods insofar as it will be processed solely for archiving purposes in the

[14] Article 5, (1) a of the GDPR.
[15] Article 5, (1) b of the GDPR.
[16] Article 29 Working Party, Opinion on Purpose Limitation, p. 4.
[17] Article 29 Working Party, Opinion on Purpose Limitation, p. 12.
[18] Article 5, (1) c of the GDPR.
[19] Article 5, (1) d of the GDPR.

public interest, scientific or historical research purposes or statistical purposes, in accordance with article 89(1).[20]

Integrity and confidentiality principle requires data to be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.[21]

In the FENTEC privacy by design approach, all data quality principles are relevant; while they may not be realized during the research phase, a privacy-by-design compliant development process will ensure that their potential exercise is facilitated in a post-project setting.

2.3.2 Accountability and general responsibility (art. 5(2) and 24)

Implementing compliance measures and being able to show compliance with the provisions of the GDPR is an important obligation of the data controller. It is contained in the second paragraph of art. 2.

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. [22]

Determining the purposes and means of data processing refers to defining the 'why and how' of the operation. The why's and how's mean determining the following:

- Adopting the decision to collect the personal data and the legal grounds to do so,
- The content of the personal data to be collected,
- The purpose(s) of the use of the collected data,
- Who are the data subjects - whose personal data will be collected,
- The possible disclosure of personal data to third parties,
- Possible restrictions to data subjects' rights, as provided for in the GDPR,
- The duration of data storage and possible future amendments to those data.[23]

The controller can do that on its own or together with other controllers, in which case they are considered joint controllers.

The general responsibility of the controller is described in art. 24.

The data controller is required to implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with the rules of the GDPR, taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons. Such measures must be reviewed and updated where necessary. This obligation may include the implementation of appropriate data protection policies, if that is proportionate to the processing activities.

[20] Article 5, (1) e of the GDPR.
[21] Article 5, (1) f of the GDPR.
[22] Article 4, (7) of the GDPR.
[23] Information Commissioner's Office, Data Controller and Data Processor: what the difference is and what the governance implications are, p. 8, available at https://ico.org.uk/media/for-organisations/documents/1546/data-controllers-and-data-processors-dp-guidance.pdf.

Adherence to approved codes of conduct as referred to in article 40 or approved certification mechanisms as referred to in article 42 may be used as an element by which to demonstrate compliance with the obligations of the controller.

2.3.3 Privacy and data protection by design and by default[24]

Data protection by design and privacy by default are among the general obligations of the controller, codified in the GDPR. They contribute to the principle of accountability, under which the data controller must be able to show its compliance with the requirements of the GDPR. Measures undertaken should be in line with the current state of the art and adopted with the aim of complying with the data controllers' obligations.[25]

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: data minimisation, purpose limitation, storage limitation and integrity and confidentiality.

The law does not provide for more specific guidelines on implementing data protection by design and by default. The appropriateness of measures required by art. 25(1) and (2) is determined on a case-by-case basis, taking into account the factors described above. Measures such as implementing security, anonymity, autonomy and transparency tools have been suggested,[26] as well as using privacy-enhancing and privacy-preserving techniques to minimise the risks toward individuals.[27]

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,[28] so it is reasonable to assume that the tenets of privacy by design also apply to article 25.

---

[24] This deliverable will use the terms privacy by design and data protection by design *interchangeably*.
[25] See Recital 78 of the GDPR.
[26] Tamò-Larrieux, A., "Interplay of Legal and Technical Privacy Protection Tools" in "Designing for Privacy and its Legal Framework", Law, Governance and Technology Series, Vol. 40, Springer, Cham.
[27] ENISA, Privacy and Data Protection by Design – from policy to engineering, 2014, p. 11.
[28] See judgments of the Court of Justice of the European Union, Joined Cases C-468/10 and C-469/10, *ASNEF and FECEMD v. Administración del Estado*, 24 November 2011, para. 42; and Joined Cases C-92/09 and C-93/09,

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.[29]

The key is therefore to focus on both legal compliance and on risks from computer enginering 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.[30]

2.3.4 Security requirements and data breach notifications

Despite FENTEC research not processing any personal data, security measures will be taken into account from the beginning of the design process, in accordance with **security by design** principle. Similarly to privacy by design, security by design means taking into account security considerations from the very beginning of the engineering process.

According to article 24 of the GDPR, the data controller is required to implement appropriate technical and organisational measures to ensure and to demonstrate that processing is performed in a GDPR-compliant manner. This obligation includes putting into place security measures, which have to be implemented according to article 32. They contribute to confidentiality, integrity and availability as security-specific goals of an IT system.[31] Privacy and security by design must not be seen as mutually exclusive. In fact, they both contribute to the same goal: a fully-functioning cyber-security system that ensures data confidentiality and security while not encroaching on the employees' private lives more than is necessary.

According to article 32 of the GDPR, the controller and the processor must implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, taking into account:

- state of the art
- the costs of implementation
- the nature, scope, context and purposes of processing
- the risk of varying likelihood and severity for the rights and freedoms of natural persons.

The measures must include, inter alia, as appropriate:

- the **pseudonymisation and encryption** of personal data; (emphasis added)
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen, para. 52. The Court deals with them together, without clearly delineating one right from another.

[29] Rubinstein, I.S., "Regulating Privacy by Design", Berkeley Technology Law Journal, 2011, Vol.26 (3), p. 1411.

[30] Tsormpatzoudi, P., Berendt, B., Coudert, F., "Privacy by Design: From Research and Policy to Practice – the Challenge of Multi-disciplinarity" in "Privacy Technologies and Policy", 2016, Vol. 9484, Springer, Cham, p. 203.

[31] ENISA, Privacy and Data protection by Design – from policy to engineering, 2014, p. 16, available at https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design.

- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.[32]

In assessing the appropriate level of security, the controller and the processor must take into account in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.[33]

This provision takes a different look on encryption – it is mentioned alongside pseudonymisation, but the two measures appear to be considered distinct. This distinction muddies the legal position of encrypted data under the GDPR, given that encryption is considered a pseudonymising measure[34].[35]

Some specific security measures suggested to ensure security by design and by default are:[36]

- no default passwords
- implement a vulnerability disclosure policy
- keep software updated
- securely store credentials and security-sensitive data
- secure communication, including separate storage of keys
- principle of least privilege
- using secure boot mechanisms to ensure software integrity
- protection of personal data
- monitoring telemetry data for security anomalies[37]

In case of a personal data breach, the controller is required to notify both the supervisory authority and the data subject.

The supervisory authority must be alerted without undue delay (if feasible, not later than 72 hours after having become aware of the breach), unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.[38] The notification must contain at least the following information:

[32] Article 32, (1) of the GDPR.
[33] Article 32, (2) of the GDPR.
[34] Spindler, G., and Schmechel, P., "Personal data and Encryption in the European General Data Protection Regulation", JIPITEC, 2016, 7, 163.
[35] In D3.2 encryption as a possible anonymization measure was discussed; since the adoption of the deliverable, the opinion of relevant expert authorities seems to indicate that encryption is firmly seen as a pseudonymising, not an anonymizing measure.
[36] Although addressed to an internet of things scenario, these measures are a good practice for security of personal data in general.
[37] UK Government - Department for digital, culture, media and sport, Code of Practice for Consumer IoT Security, 2018, available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/773867/Code_of_Practice_for_Consumer_IoT_Security_October_2018.pdf .
[38] Article 33, (1) of the GDPR.

- describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
- communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
- describe the likely consequences of the personal data breach;
- describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.[39]

If it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.[40]

The controller must document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with article 33.[41]

The data subject must be informed without undue delay if the breach is likely to result in a high risk to the rights and freedoms of natural persons. The breach must be communicated in clear language and include at least the information mentioned in the above alineas.

There is no need to inform the data subject if:

- the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;
- the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;
- it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

Meeting one of the conditions is enough for the notification duty to not apply.[42]

However, the supervisory authority may require the controller to notify the data subject, if it considers the personal data breach likely to result in a high risk.[43]

The processor also has the duty of notification, namely it must notify the controller without undue delay after becoming aware of a personal data breach.[44]

2.3.5 Data protection impact assessment

Under the Directive 95/46/EC, data controllers were required to notify competent authorities if they were processing personal data. While that obligation produced extra administrative and financial burdens, it did not in all cases contribute to improving the protection of personal data. Therefore, the

[39] Article 33, (3) of the GDPR.
[40] Article 33, (4) of the GDPR.
[41] Article 33, (5) of the GDPR.
[42] Article 34, (2) of the GDPR.
[43] Article 34, (3) of the GDPR.
[44] Article 33, (2) of the GDPR.

GDPR abolished such indiscriminate general notification obligations, and instead replaced them by effective procedures and mechanisms which focus instead on those types of processing operations which are likely to result in a high risk to the rights and freedoms of natural persons by virtue of their nature, scope, context and purposes. In such cases, **a data protection impact assessment (DPIA)** should be carried out by the controller prior to the processing in order to assess the particular likelihood and severity of the high risk, taking into account the nature, scope, context and purposes of the processing and the sources of the risk. That impact assessment should include, in particular, the measures, safeguards and mechanisms envisaged for mitigating that risk, ensuring the protection of personal data and demonstrating compliance with the GDPR.[45]

This means that the GDPR adopted a risk-based approach: only certain processing operations, which pose a high risk, necessitate adoption of a DPIA. More specifically, carrying out a DPIA is required in three situations:

(1) The data controller is explicitly required to do so by the GDPR in the following cases:
   a. a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
   b. processing on a large scale of special categories of data referred to in article 9(1), or of personal data relating to criminal convictions and offences referred to in article 10; or
   c. a systematic monitoring of a publicly accessible area on a large scale.[46]

(2) If the processing activity is on the list, published by the national supervisory authority.[47]

(3) If the processing is likely to result in a high risk to the rights and freedoms of natural persons, especially if new technologies are used.[48]

According to article 35(7), a DPIA must contain at least the following:

- 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 1; and
- 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 this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

[45] Recitals 89 and 90 of the GDPR.
[46] Article 35, (3) of the GDPR.
[47] Article 35, (4) of the GDPR.
[48] Article 35, (1) of the GDPR.

The contents of a DPIA are further specified by the Article 29 Working Party's Opinion: [49][50]

1. Systematic description

Data controllers must define and take into account the *nature, scope, context and purpose* of processing, according to Recital 90 of the GDPR; they all refer to setting up a cyber-secure system within an LPA. The description of the processing operation must be functional.

Next, it must describe which personal data will be processed in this operation.

Another requirement is identification of the assets, on which personal data rely, such as software, hardware, networks, people, paper or paper transmission channels.

Finally, this section must take into account potential compliance with approved codes of conduct.

2. Proportionality and necessity

When assessing proportionality and necessity according to article 35(7)b and Recital 90, the data controller must take into account the following: on the one hand, measures contributing to the proportionality and the necessity of the processing, based on the principles of data processing, and on the other hand, measures contributing to the rights of the data subject.

The principles that must be taken into account, are specified, explicit and legitimate purpose; lawfulness of processing, data minimisation and storage limitation.

Measures must contribute to rights such as the right to be informed according to articles 12, 13 and 14 of the GDPR, the right of access and portability, the right to rectify, erase, object to and restrict processing. They must also include the definition of recipient(s) of personal data, and processor, if applicable. In case of transfer of data to third countries, they must include certain safeguards. Prior consultation with the competent authority according to article 36 of the GDPR must also be considered.

3. Risk management

Risk management section of a DPIA must address the risks to the rights and freedoms of data subjects, specifically it must define the origin, nature, particularity and severity of the risks. For risks, such as *illegitimate access, undesired modification, and disappearance of data*, it must, from the perspective of the data subjects, take into account the risk sources, potential impact on the rights and freedoms of natural persons, potential threats that could lead to such risks, as well as their likelihood and severity.

It must also determine measures, envisaged to treat those risks.

4. Involvement of interested parties

In order to protect legitimate interests of interested parties, the data controller must seek the advice of the data protection officer when carrying out the DPIA, as well as seek the views of data subjects or their representatives, if appropriate. This means consulting the representatives of employees as well as

[49] This section is wholly based on Article 29 Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, WP 248.

[50] This opinion has been endorsed by the EDPB, which replaced the previous body on May 25 2018.

citizens. Such consultation is inappropriate if it harms the protection of commercial or public interests or the security of processing operations.[51]

Data controllers are responsible to ensure that a DPIA is carried out when the processing operation is likely to result in a high risk to the rights and freedoms of natural persons, especially if new technologies are used. High risk is thus the deciding criterion for necessity of an DPIA. The guidelines provide a non-exhaustive list of criteria to identify high risk, such as evaluation or scoring, including profiling and predicting; systematic monitoring, combined or matched datasets etc. [52]

It is unlikely that FENTEC use-cases will pose significant high risks in the sense of the Opinion. Nevertheless, the need to conduct a DPIA will be identified in the final deliverable D3.4, and if necessary, the DPIA will be performed in its due course.

2.4 Legal requirements from the cybersecurity framework

The Cybersecurity Act[53], which entered into force on the 27th of June 2019, provides an EU framework for cybersecurity in order to improve the conditions of the internal market and to improve cybersecurity in a broad range of digital products and services. This framework will establish European cybersecurity certification schemes (ECCSs) that aim at increasing the quality of European products and services with a seal that will guarantee their level of cybersecurity. With these measures the EU hopes to ensure the secure transmission and storage of data, thereby bolstering the security of critical infrastructures against cyber threats and protecting societies' most essential services.[54]

The Cybersecurity Act states that the Commission shall publish a Union rolling working programme in order to identify strategic priorities for future ECCSs. This programme will also include a list of ICT products, services, and processes or categories thereof that are capable of falling under the scope of the ECCS.[55]

The developed ECCS shall aim to achieve, at minimum, a set of security objectives. These objectives include, among others; the protection of data against unauthorized storage, access, destruction, and alteration, the identification or documentation of known dependencies and vulnerabilities, checking which data, services, and functions have been accessed or used (incl. at what times and by whom), etc.[56] The ECCS shall also include, at minimum, the series of elements listed in article 54 of the Cybersecurity Act (f.e. rules on how previously undetected cybersecurity vulnerabilities are reported and dealt with, conditions for mutual recognition of certification schemes with third countries, etc.).[57] Additionally, the

[51] Article 35, (9) of the GDPR.

[52] Article 29 Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, WP 248.

[53] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).

[54] S., Stolton, "The EU's search for tough cybersecurity standards, 12 September 2019, https://www.euractiv.com/section/cybersecurity/news/the-eus-search-for-tough-cybersecurity-standards/ (last accessed 8 December, 2019).

[55] Article 46, 2 and 47 of the Cybersecurity Act.

[56] Article 51 of the Cybersecurity Act.

[57] Article 54 of the Cybersecurity Act.

manufacturer or provider of a certified ICT product, service, or process must make publicly available specific supplementary information.[58]

An ECCS may also specify one or more assurance levels for ICT products, services, and processes. These assurance levels correspond to the level of risk related to the intended use of the ICT product, service, or process.[59] The assurance levels can be summarized as follows:

1. Basic level: intended to minimize the known basic risks of incidents and cyberattacks. The evaluation activities shall include at least a review of technical documentation.[60] ICT products, services, and processes of this level may be subject to a conformity self-assessment by the manufacturer or provider.[61]
2. Substantial level: intended to minimize the known cybersecurity risks, and the risk of incidents and cyberattacks carried out by actors with limited skills and resources. The evaluation activities shall include at least a review to demonstrate the absence of publicly known vulnerabilities and testing to demonstrate the correct implementation of security functionalities.[62]
3. High level: intended to minimize the risk of state-of-the art cyberattacks carried out by actors with significant skills and resources. The evaluation activities shall be the same as under the 'substantial level', in addition to an assessment of the resistance to skilled attackers, using penetration testing. [63]

[58] Article 55 of the Cybersecurity Act.
[59] Article 52, 1 of the Cybersecurity Act.
[60] Article 52, 5 of the Cybersecurity Act.
[61] Article 53 of the Cybersecurity Act.
[62] Article 52, 6 of the Cybersecurity Act.
[63] Article 52, 7 of the Cybersecurity Act.

3 Digital currency scenario

The use-case by ATOS concerns the use of a privacy-preserving digital currency. More specifically, a payment system will be designed, which will prevent the coins used from being traceable back to the entity which claimed them. Since the inability to link the payer and payee may cause difficulties in detecting money laundering and tax evasion by governments and internal auditing agencies, the system will be designed with an option to restore traceability using an escrow mechanism. The resulting mechanism will allow for different transactions, including daily transactions, such as microtransactions and payments to friends and businesses; payments resulting in a tax declaration with possible automated deductions, based on certain types of expenses; and special purpose coins, i.e. monies that can only be spent on certain products or services, typically child benefit payments or meal vouchers.

The payment will be carried out in three steps: first the customer needs to retrieve (or give back) digital currency, then the coins are spent in a transaction, and finally data of the transaction are stored and made auditable.[64]

In this use-case, the different applications and possible conflicts of e-finance legislation on payment services and preventing money laundering, with legislation on data protection, are examined. Functional encryption serves as a security measure in protecting personal data and contributes to proportionality and balancing the amount of personal and payment data visible to the auditing authority.

[64] For a comprehensive description of use-cases and requirements, see D7.1 and D3.1, respectively.

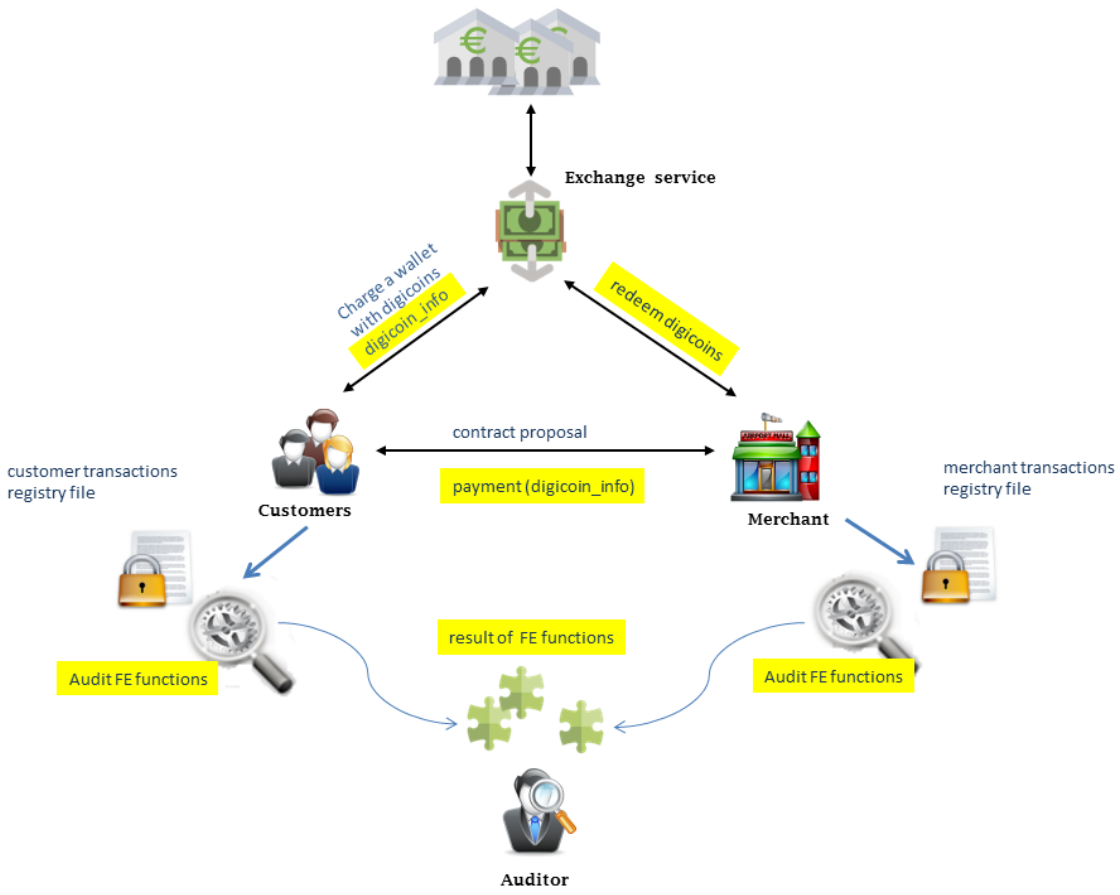

Figure 1: Digital currency scenario (source: D3.1)

The payment system, devised in this use-case, is likely to fall under several pieces of legislation on EU level. As described in D3.2, these legal instruments are the Second E-money Directive (2009/110/EC), the Second Payment Services Directive (2015/2366), and the Anti-Money Laundering Directive (2015/849). In this section, their obligations and requirements, especially those relevant to security and authentication, will be examined.

3.1 Second E-money Directive (2009/110/EC)

The Second E-Money Directive (EMD2) was adopted in 2009 in order to level the playing field in regulating the electronic money issuers.[65] The full applicability and potential relevance of the EMD2 for FENTEC use-case was examined in D3.2.

[65] See Recitals 3 and of the EMD2, as well as N. VANDEZANDE, *Virtual Currencies: A Legal Framework*, Cambridge, Intersentia, 2018, for a full and comprehensive overview.

The EMD2 applies to '*electronic money issuers*'. In the digital currency scenario, they are likely to be credit institutions (as recognised under the CRD IV [Directive 2013/36/EU]) or electronic money institutions, regulated in this Directive.[66]

Since the EMD2 deals with requirements to take up and pursue, and supervise e-money issuers, any privacy, security and authentication obligations must be deduced from other legislation, especially the GDPR, and regulation of payment services and money laundering.

3.2 Second Payment Services Directive (2015/2366)

The Second Payment Services Directive (PSD II) is a full harmonization instrument, with limited exceptions, aiming to close the regulatory gaps while at the same time providing more legal clarity and ensuring consistent application of the legislative framework across the Union. Among other goals, it addresses the security challenges of ever more complex online payments. In its Recital 7, it states that safe and secure payment services constitute a vital condition for a well-functioning payment services market. Users of payment services should therefore be adequately protected against such risks. In its Recitals 68 and 69, it endorses the use of authentication measures, especially in an online environment, and sets out the need to keep those credentials secure.

The PSD II applies to '*payment services*' provided by payment service providers (PSPs).

Payment services are listed in Annex I of the Directive. The list is exhaustive, which means that any kind of monetary transaction or transfer that is not mentioned in it, cannot be considered a payment service and does therefore not fall under the scope of the Directive.

Payment services providers are entities, that fall into any of the following six categories: (1) credit institutions,[67] (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). For purposes of FENTEC project, the most relevant types of payment services providers are credit institutions as possible adopters of the digital currency payment system, and electronic money institutions, as described in the above chapter on e-money regulation.

While the full scope and applicability was discussed in deliverable D3.2, here we briefly draw attention to a possibly relevant scope exemption, contained in art. 3(k) of the PSD2, which exempts 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;

[66] Article 1, 1 of Directive 2009/110/EC.
[67] As defined in point (1) of article 4, (1) of Regulation (EU) No 575/2013.

(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;

However, at this stage of the use-case development, it is not possible to say with certainty whether the planned digital coin meets any of these criteria. Given its commercial, for-profit nature, the coin is likely to be usable more widely than in the foreseen exemption.

In this phase of project research, it is important to discuss the authorisation, authentication and security measures of the PSD II.

Authentication is defined in art. 4(2) as a procedure which allows the payment service provider to verify the identity of a payment service user or the validity of the use of a specific payment instrument, including the use of the user's personalised security credentials

Strong customer authentication (art. 4(30)) means an authentication based on the use of two or more elements categorised as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is) that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data.

Personalised security credentials (art. 4(31)) are defined as personalised features provided by the payment service provider to a payment service user for the purposes of authentication.

Sensitive payment data (art. 4(32)) are data, including personalised security credentials which can be used to carry out fraud. For the activities of payment initiation service providers and account information service providers, the name of the account owner and the account number do not constitute sensitive payment data.

3.2.1 Authorisation of payment transactions

Consent and withdrawal of consent (art. 64)

Payment transactions can only be considered authorised if the payer has consented to its execution. The consent must usually be given prior to the execution of the payment, unless there is an explicit agreement between the payer and the payment provider that the consent can be given after the execution. The form of the consent must be agreed in advance between the parties; it can also be given via the payee or the payment initiation service provider. In the absence of consent, a payment transaction shall be considered to be unauthorised.

Consent may also be withdrawn. However, there is a time limit: once the payment order has been received by the payer's payment service provider, withdrawal of consent is no longer effective, according to art. 80 ("irrevocability"). Consent to execute a series of payment transactions may also be withdrawn, in which case any future payment transaction shall be considered to be unauthorised.

Rules on access to payment account in the case of payment initiation services (art. 66) and in the case of payment account information in the case of account information services (art. 67)

Payment initiation services providers typically help consumers to make online credit transfers and inform the merchant immediately of the payment initiation, allowing for the immediate dispatch of goods or immediate access to services purchased online. For online payments, they constitute a true alternative to credit card payments as they offer an easily accessible payment service, as the consumer only needs to possess an online payment account.[68]

This and the following provisions of the PSD2 'opened the door' to open banking by requiring banks to grant third parties access to payment accounts based on consumer's consent, with the aim of promoting market competition.[69]

Account information services allow consumers and businesses to have a global view on their financial situation, for instance, by enabling consumers to consolidate the different payment accounts they may have with one or more banks and to categorise their spending according to different typologies (food, energy, rent, leisure, etc.), thus helping them with budgeting and financial planning.[70]

Alongside traditional payment services providers, such as banks, payment initiation services providers and account information services providers can also request access to information about the payment account. This means accessing the payer's information, including personal data, insofar as the payer is covered by the GDPR. In order to prevent excessive screenscraping, PSD regulates data access of both entities. The rules apply only in an online environment.

(1) Rules on access for payment initiation services providers

According to art. 66(3), the payment initiation service provider shall:

- not hold at any time the payer's funds in connection with the provision of the payment initiation service;
- ensure that the personalised security credentials of the payment service user are not, with the exception of the user and the issuer of the personalised security credentials, accessible to other parties and that they are transmitted by the payment initiation service provider through safe and efficient channels;
- ensure that any other information about the payment service user, obtained when providing payment initiation services, is only provided to the payee and only with the payment service user's explicit consent;
- every time a payment is initiated, identify itself towards the account servicing payment service provider of the payer and communicate with the account servicing payment service provider, the payer and the payee in a secure way, in accordance with point (d) of article 98(1);[71]

[68] European Commission, Payment Services Directive: frequently asked questions, Factsheet. 12 January 2018. https://europa.eu/rapid/press-release_MEMO-15-5793_en.htm?locale=en.

[69] The European Consumer Organisation, "BEUC's recommendations to the EDPB on the interplay between the GDPR and PSD2", 2019, available at https://www.beuc.eu/publications/beuc-x-2019-021_beuc_recommendations_to_edpb-interplay_gdpr-psd2.pdf.

[70] European Commission, Payment Services Directive: frequently asked questions, Factsheet. 12 January 2018. https://europa.eu/rapid/press-release_MEMO-15-5793_en.htm?locale=en.

[71] Art. 98(1)(d) states that

1. EBA shall, in close cooperation with the ECB and after consulting all relevant stakeholders, including those in the payment services market, reflecting all interests involved, develop draft regulatory technical standards

- not store sensitive payment data of the payment service user;
- not request from the payment service user any data other than those necessary to provide the payment initiation service;
- not use, access or store any data for purposes other than for the provision of the payment initiation service as explicitly requested by the payer;
- not modify the amount, the payee or any other feature of the transaction.

As soon as the payer gives its explicit consent for a payment to be executed, the account servicing payment service provider shall perform the following actions in order to ensure the payer's right to use the payment initiation service (art. 66(4):

- communicate securely with payment initiation service providers in accordance with point (d) of article 98(1);
- immediately after receipt of the payment order from a payment initiation service provider, provide or make available all information on the initiation of the payment transaction and all information accessible to the account servicing payment service provider regarding the execution of the payment transaction to the payment initiation service provider;
- treat payment orders transmitted through the services of a payment initiation service provider without any discrimination other than for objective reasons, in particular in terms of timing, priority or charges vis-à-vis payment orders transmitted directly by the payer.

The provision of payment initiation services is independent of the existence of a contractual relationship between the payment initiation service providers and the account servicing payment service providers for that purpose.

(2) Rules on access for account information services providers

The payment services user has the right to make use of services enabling access to account information in an online environment.

The account information service provider shall:

- provide services only where based on the payment service user's explicit consent;
- ensure that the personalised security credentials of the payment service user are not, with the exception of the user and the issuer of the personalised security credentials, accessible to other parties and that when they are transmitted by the account information service provider, this is done through safe and efficient channels;
- for each communication session, identify itself towards the account servicing payment service provider(s) of the payment service user and securely communicate with the

addressed to payment service providers as set out in article 1(1) of this Directive in accordance with article 10 of Regulation (EU) No 1093/2010 specifying:

...

(d) the requirements for common and secure open standards of communication for the purpose of identification, authentication, notification, and information, as well as for the implementation of security measures, between account servicing payment service providers, payment initiation service providers, account information service providers, payers, payees and other payment service providers.

account servicing payment service provider(s) and the payment service user, in accordance with point (d) of article 98(1);
- access only the information from designated payment accounts and associated payment transactions;
- not request sensitive payment data linked to the payment accounts;
- not use, access or store any data for purposes other than for performing the account information service explicitly requested by the payment service user, in accordance with data protection rules.

In relation to payment accounts, the account servicing payment service provider shall:

- (a) communicate securely with the account information service providers in accordance with point (d) of article 98(1); and
- (b) treat data requests transmitted through the services of an account information service provider without any discrimination for other than objective reasons.

Similarly to the previous article, art. 67(4) does not require the existence of a contractual relationship between the account information service providers and the account servicing payment service providers in order to provide account information services.

Obligations of the payment service user in relation to payment instruments and personalised security credentials (art. 69)

This article lays down the rules for users of payment instruments. According to the first paragraph, the user must use the payment instrument in accordance with the terms governing the issue and use of the payment instrument, which must be objective, non-discriminatory and proportionate; and notify the payment service provider of the loss, theft, misappropriation or unauthorised use of the payment instrument. The user must do so without undue delay on becoming aware of the incident.

The user must, in particular, take all reasonable steps to keep its personalised security credentials safe, for example, in a digital currency scenario, not disclose the PIN code in case of a physical instrument, or username/password in an online environment.

Obligations of the payment service provider in relation to payment instruments (art. 70)

The payment service provider issuing a payment instrument is required to ensure that the personalised security credentials are only accessible to the entitled user, refrain from sending an unsolicited payment instrument, and ensure the user can at all times, free of charge, report the loss, theft, misappropriation or unauthorised use of the payment instrument.

The risk of sending a payment instrument or any personalised security credentials to the user must be borne by the payment services provider.

Notification and rectification of unauthorised or incorrectly executed payment transactions (art. 71)

If the payment was executed without authorisation or incorrectly, the payment service user can only ask for rectification if he or she has notified payment service provider without undue delay on becoming aware of any such transaction, and no later than 13 months after the debit date.

Evidence on authentication and execution of payment transactions (art. 72)

Where a payment service user denies having authorised an executed payment transaction or claims that the payment transaction was not correctly executed, it is for the payment service provider to prove that the payment transaction was authenticated, accurately recorded, entered in the accounts and not affected by a technical breakdown or some other deficiency of the service provided by the payment service provider.

If the payment transaction is initiated through a payment initiation service provider, the burden shall be on the payment initiation service provider to prove that within its sphere of competence, the payment transaction was authenticated, accurately recorded and not affected by a technical breakdown or other deficiency linked to the payment service of which it is in charge.

This obligation is homologous to art. 30 of the GDPR (keeping records) insofar as the payment service provider acts as a data controller with insight into the user's personal data.

Payment service provider's liability for unauthorised payment transactions (art. 73)

This requirements relates to the obligation to keep security credentials safe and secure. If an unauthorised payment is carried out, the payer's payment service provider refunds the payer the amount of the unauthorised payment transaction immediately, and in any event no later than by the end of the following business day, after noting or being notified of the transaction, except where the payer's payment service provider has reasonable grounds for suspecting fraud and communicates those grounds to the relevant national authority in writing. Where applicable, the payer's payment service provider shall restore the debited payment account to the state in which it would have been had the unauthorised payment transaction not taken place. This shall also ensure that the credit value date for the payer's payment account shall be no later than the date the amount had been debited.

3.2.2 Operational and security risks and authentication

Management of operational and security risks (art. 95)

PSPs are required to establish a framework with appropriate mitigation measures and control mechanisms to manage the operational and security risks, relating to the payment services they provide. As part of that framework, they must establish and maintain effective incident management procedures, including for the detection and classification of major operational and security incidents. An updated and comprehensive assessment of the operational and security risks and on the adequacy of the mitigation measures and control mechanisms implemented to counter them must be reported to the competent authority on a regular basis.

This article also grants the European Banking Authority (EBA) competence to adopt guidelines with regard to the establishment, implementation and monitoring of the security measures, including certification processes where relevant.

The notion of major operational and security incident is explained by the EBA in its Guidelines on major incident reporting.[72] The guidelines apply to all incidents included under the definition of 'major operational or security incident', which covers both external and internal events that could be either malicious or accidental. These guidelines apply also where the major operational or security incident originates outside the Union (e.g. when an incident originates in the parent company or in a subsidiary established outside the Union) and affects the payment services provided by a payment service provider located in the Union either directly or indirectly (the capacity of the payment service provider to keep carrying out its payment activity is jeopardised in some other way as a result of the incident). The guidelines define a *major operational or security incidents as "a singular event or a series of linked events unplanned by the payment service provider which has or will probably have an adverse impact on the integrity, availability, confidentiality, authenticity and/or continuity of payment related services*".[73]

Other relevant documents by the EBA include the Guidelines on the security measures for operational and security risks of payment services,[74] and Regulatory Technical Standards (RTS) on strong customer authentication and common and secure communication under PSD2.[75][76] Since both sets of guidelines are given on a technical rather than legal level, though the latter is also given due consideration, they will not be further explained here.

Incident reporting (art. 96)

In the case of a major operational or security incident, payment service providers shall, without undue delay, notify the competent authority in the home Member State of the payment service provider. Where the incident has or may have an impact on the financial interests of its payment service users, the payment service provider shall, without undue delay, inform its payment service users of the incident and of all measures that they can take to mitigate the adverse effects of the incident.

This provision ties in with article 34 of the GDPR, which requires data controllers to notify competent authorities and data subjects about breaches of personal data, unless certain criteria are met, as well as notifying a significant disruptive effect under article 14 of the NIS Directive.

[72] The European Banking Authority, "Guidelines on major incident reporting under PSD2 (EBA/GL/2017/10)", available at https://eba.europa.eu/eba-publishes-final-guidelines-on-major-incident-reporting-under-psd2.

[73] See also reply by EBA, no. 2018_4144.

[74] Available at https://eba.europa.eu/sites/default/documents/files/documents/10180/2060117/d53bf08f-990b-47ba-b36f-15c985064d47/Final%20report%20on%20EBA%20Guidelines%20on%20the%20security%20measures%20for%20operational%20and%20security%20risks%20under%20PSD2%20(EBA-GL-2017-17).pdf.

[75] The European Banking Authority, "Regulatory Technical Standards (RTS) on strong customer authentication and common and secure communication under PSD2 (EBA/RTS/2017/02)", available at https://eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/regulatory-technical-standards-on-strong-customer-authentication-and-secure-communication-under-psd2 .

[76] RTS were also adopted as a Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication.

Authentication (art. 97)

Under the PSD2, strong authentication is required for accessing payment accounts online, initiating electronic payment transactions and carrying out any action through a remote channel which may imply a risk of payment fraud or other abuses. Payment service providers, including banks, must have in place adequate security measures to protect the confidentiality and integrity of payment service users' personalised security credentials. For electronic remote payment transactions, payment service providers apply strong customer authentication that includes elements which dynamically link the transaction to a specific amount and a specific payee.

A payment service provider must apply strong customer authentication where the payer:

(a) accesses its payment account online;

(b) initiates an electronic payment transaction;

(c) carries out any action through a remote channel which may imply a risk of payment fraud or other abuses.

PSPs must apply strong customer authentication that includes elements which dynamically link the transaction to a specific amount and a specific payee for electronic remote payment transactions. They must put in place adequate security measures to protect the confidentiality and integrity of payment service users' personalised security credentials.

The notion of strong customer authentication (SCA) was recently further explained in so-called Regulatory Technical Standards (RTS), adopted on by the Commission on the basis of European Banking Authority's activities (Commission delegated regulation 2018/389.). SCA is described as a *procedure* (art. 1(a), emphasis added), implying that it is a dynamic rather than static notion. In order to comply with SCA, payment provider must ensure that authentication is based on two or more elements factors. They are categorised as knowledge, possession and inherence. In other words: in order to access a payment service, identity will be ascertained based on at least two of the following factors - something you know (e.g. a password or a PIN), something you have (e.g. confirmation through a second device – Google already does something similar for accessing Gmail on untrusted devices), or something you are (e.g. biometrics). There are some exceptions to requiring two-step factor authentication, for example for transactions below EUR 30.

The RTS were adopted based on art. 98, which gives EBA the competence to do so.

3.2.3 Relationship with the GDPR

Data protection in payment services is the subject of Recital 89, and article 94 of the PSD2. While other articles, especially those on access to information by payment services providers, arguably contain a broad link to data protection law, this is the only explicit rule on the subject.

Processing of personal data by payment systems and payment service providers is only permitted when necessary to safeguard the prevention, investigation and detection of payment fraud. The provision of information to individuals about the processing of personal data and the processing of such personal data and any other processing of personal data for those purposes must be done in accordance with the GDPR (in the original text: Directive 95/46). Payment service providers shall only access, process and

retain personal data necessary for the provision of their payment services, with the explicit consent of the payment service user.[77]

The notions of consent under the GDPR and explicit consent under the PSD2, do not necessarily overlap. It has been argued that explicit consent might not even be necessary insofar as the PSP relies on other legal grounds to process personal data, such as necessary for the fulfilment of a contract between them – i.e. to provide a payment initiation or account information service. Since other legal grounds are provided, consent should not be asked despite the PSD2's requirement.[78]

The Bureau Européen des Unions de Consommateurs (BEUC) report has identified several questions about the relationship between the GDPR and PSD2:[79]

1. [Informed] consent versus explicit consent: where PSD2 requires explicit consent, it should be held to the same standard as required by the GDPR. Moreover, consumers – users of payment services that are also data subjects – should be fully aware of what they are consenting to and that their data protection rights apply
2. Silent party data processing: when payment services are provided by a third party provider, measures should be taken not to unduly disclose personal data – the question of legitimate interests (carrying out payments/enabling account information services) as legal grounds, and may we add – also questions of data minimisation and purpose limitation
3. Profiling and automated decision-making: GDPR rules that apply to special categories of data and automated decision-making, including profiling, are highly relevant to and fully apply in the PSD2 context. In such cases, the highest standards of explicit consent must be adhered to
4. Data quality principles: respect data minimisation and data security: different actors (traditional payment services providers, such as banks; account information services and payment information services) should have access to different amounts and types of data based on the (strict) necessity of access. Authentication is not consent.
5. Processing of sensitive data/special categories of data: payment history can reveal a lot of information pertaining to e.g. health status. Only explicit consent may be legal grounds for their processing, and consumers should be able to select which data they wish to share with payment services providers.

Those recommendations were adopted by the then-Article 29 Working Party (now European Data Protection Board, or EDPB) in their letter to Member of the European Parliament (MEP) In 't Veld.[80] Moreover, the WP29 suggests **Regulatory Technical Standards**, issues by the European Banking Authority (EBA), must be taken into account when adopting technical and organisational security measures, and that **interfaces** designed by banks **to facilitate data access** must take into account both the European competition law framework and article 32 of the GDPR (security of processing). The letter

[77] Art. 94/1, 2 of the PSD2.
[78] Vandezande, N., "Reconciling Consent in PSD2 and GDPR", 2019, accessible at https://thepaypers.com/expert-opinion/reconciling-consent-in-psd2-and-gdpr--777976 .
[79] The European Consumer Organisation, "BEUC'S recommendations to the EDPB on the interplay between the GDPR and PSD2", 2019, available at https://www.beuc.eu/publications/beuc-x-2019-021_beuc_recommendations_to_edpb-interplay_gdpr-psd2.pdf.
[80] https://edpb.europa.eu/sites/edpb/files/files/file1/psd2_letter_en.pdf .

also foresees the potential need for future collaboration between European data protection and financial supervisory bodies.

3.2.4 Other relevant obligations

3.2.4.1 Transparency and information requirements

Under Title III, Transparency of conditions and information requirements for payment services, PSPs are required to provide users with certain information, on principle free of charge (art. 40). The payment service provider must be able to prove that it has supplied the user with the necessary information – it carries the *burden of proof* (art. 41). The rules on provision of information apply to single payment transactions, framework contracts and payment transactions covered by them. If the payment service user is not a consumer parties may agree that it shall not apply in whole or in part.

Different information must be given at different times, depending on the service and timing. Since it is unclear who will play what kind of role in the digital currency scenario, we break down all the possibilities and requirements, to be applied as relevant.

Prior general information and conditions (art. 44 and 45)

Before the payment service user is bound by a single payment service contract or offer, the payment service provider is required to make available to the payment service user, in an easily accessible manner, the following information and conditions, specified in article 45:

(a) a specification of the information or unique identifier to be provided by the payment service user in order for a payment order to be properly initiated or executed;
(b) the maximum execution time for the payment service to be provided;
(c) all charges payable by the payment service user to the payment service provider and, where applicable, a breakdown of those charges;
(d) where applicable, the actual or reference exchange rate to be applied to the payment transaction.

Moreover, the payment initiation service providers shall, prior to initiation, provide the payer with, or make available to the payer, the following clear and comprehensive information:

(a) the name of the payment initiation service provider, the geographical address of its head office and, where applicable, the geographical address of its agent or branch established in the Member State where the payment service is offered, and any other contact details, including electronic mail address, relevant for communication with the payment initiation service provider; and
(b) the contact details of the competent authority.

Information for the payer and payee after the initiation of a payment order (art. 46)

In addition to the information and conditions specified in article 45, where a payment order is initiated through a payment initiation service provider, the payment initiation service provider shall, immediately after initiation, provide or make available all of the following data to the payer and, where applicable, the payee:

(a) confirmation of the successful initiation of the payment order with the payer's account servicing payment service provider;

(b) a reference enabling the payer and the payee to identify the payment transaction and, where appropriate, the payee to identify the payer, and any information transferred with the payment transaction;
(c) the amount of the payment transaction;
(d) where applicable, the amount of any charges payable to the payment initiation service provider for the transaction, and where applicable a breakdown of the amounts of such charges.

Information for the payer after receipt of the payment order (art. 48)

Immediately after receipt of the payment order, the payer's payment service provider shall provide the payer with or make available to the payer, in the same way as provided for in article 44(1), all of the following data with regard to its own services:

(a) a reference enabling the payer to identify the payment transaction and, where appropriate, information relating to the payee;
(c) the amount of the payment transaction in the currency used in the payment order;
(d) the amount of any charges for the payment transaction payable by the payer and, where applicable, a breakdown of the amounts of such charges;
(e) where applicable, the exchange rate used in the payment transaction by the payer's payment service provider or a reference thereto, when different from the rate provided in accordance with point (d) of article 45(1), and the amount of the payment transaction after that currency conversion;
(f) the date of receipt of the payment order.

Information for the payee after execution (art. 49)

Immediately after the execution of the payment transaction, the payee's payment service provider shall provide the payee with, or make available to, the payee, in the same way as provided for in article 44(1), all of the following data with regard to its own services:

(a) a reference enabling the payee to identify the payment transaction and, where appropriate, the payer and any information transferred with the payment transaction;
(b) the amount of the payment transaction in the currency in which the funds are at the payee's disposal;
(c) the amount of any charges for the payment transaction payable by the payee and, where applicable, a breakdown of the amounts of such charges;
(d) where applicable, the exchange rate used in the payment transaction by the payee's payment service provider, and the amount of the payment transaction before that currency conversion;
(e) the credit value date.

3.2.5 Liability

Article 20 lays down the rules for liability in payment services.

If payment institutions rely on third parties for the performance of operational functions, those payment institutions take reasonable steps to ensure that the requirements of this Directive are complied with. Payment institutions remain fully liable for any acts of their employees, or any agent, branch or entity to which activities are outsourced.

3.3 Fourth and Fifth Anti-money Laundering Directives (2015/849 and 2018/843)

The goal of monitoring and preventing money laundering is to put serious obstacles in the path of organised serious crime and terrorism. Recent updates of the anti-money laundering legal framework in the EU have followed the adaptation of Financial Action Task Force's 2012 Guidelines, resulting in the Fourth (MLD IV) and Fifth Anti-Money Laundering Directives (MLD V) in 2015 and 2018, respectively. While the previous iterations of the MLD were rules-based, the MLD IV introduced a risk-based approach, followed also in the MLD V.[81] This means that entities, bound by the MLD's rules must adopt measures, appropriate to the risks posed by a customer or a transaction.

Various important obligations to the end of preventing money laundering are carrying out a due diligence procedure, also known as know your client (KYC), reporting to competent authorities, and retaining data. However, these requirements also pose questions relating to privacy and protection of personal data, processed in the aim of attaining the goal. European law must abide by the principle of proportionality, as laid out in article 52(1) of the Charter of Fundamental Rights:

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.

MLD's sweeping data processing and retention powers are regarded by some authors to be too broad to comply with this principle. Namely, since 94% of Europeans are in some involved in the financial system and any transaction could potentially be regarded as suspicious, there is a risk of general, non-purposeful data collection in lead-up to mass surveillance.[82] Therefore, this section will also touch upon the relationship between MLD and GDPR in order to comment on these views.

3.3.1 Scope

'*Money laundering*' is defined in article 1(3) of the MLD 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;

[81] Steenwijk, P., "A Balanced Package: Fighting Money Laundering with the 4th European Directive" in De Zwaan, J., Lak, M., Makinwa, A., Willems, P. (eds), *Governance and Security Issues of the European Union*, T.M.C. Asser Press, The Hague, 2016.

[82] Milaj, J., Kaiser, C., "Retention of data in the new Anti-money Laundering Directive—'need to know' versus 'nice to know'", International Data Privacy Law, Vol. 7, Issue 2, May 2017, Pages 115–125, https://doi.org/10.1093/idpl/ipx002.

(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."[83]

The following entities are bound by the MLD IV's rules, regardless of their status (legal or natural person), as long as they are acting in their professional activities:

- auditors, external accountants and tax advisors;
- notaries and other independent legal professionals, regarding certain financial transactions,
- trust or company service providers not already covered under point (a) or (b);
- estate agents;
- other persons trading in goods to the extent that payments are made or received in cash in an amount of EUR 10 000 or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked;
- providers of gambling services.

MLD V has extended this scope – it also applies to the following subjects:

- providers engaged in exchange services between virtual currencies and fiat currencies; virtual currencies are defined as a "digital representation of value that can be digitally transferred, stored or traded and is accepted… as a medium of exchange"
- custodian wallet providers;
- persons trading or acting as intermediaries in the trade of works of art, including when this is carried out by art galleries and auction houses, where the value of the transaction or a series of linked transactions amounts to EUR 10 000 or more;
- persons storing, trading or acting as intermediaries in the trade of works of art when this is carried out by free ports, where the value of the transaction or a series of linked transactions amounts to EUR 10 000 or more.

Thus, digital and virtual currencies, such as bitcoins, are also covered by the anti-money laundering regulations and their issuers and custodians must likewise report to competent financial authorities. The digital coin developed in the FENTEC use-case will most likely be a "regular" currency, as opposed to a virtual one in the sense of MLD V, and falling fully under its regime.

3.3.2 Politically exposed persons

Anti-money laundering regulation is based on the assumption that individuals holding high political office may be at larger risk of bribery or corruption by the virtue of the office entrusted to them. Financial Action Task Force on Money Laundering (FATF) defines a politically exposed person (PEP) as an "individual who is or has been entrusted with a prominent public function". Potential risks associated

[83] Article 3, (3) of Directive (EU) 2015/849.

with PEPs justify the application of additional preventive measures in scrutinising business relationships and addressing abuses, if they occur.[84]

In the MLD IV and MLD V, a PEP is defined as a natural person who is or who has been entrusted with prominent public functions and includes the following:

- heads of state, heads of government, ministers and deputy or assistant ministers;
- members of parliament or of similar legislative bodies;
- members of the governing bodies of political parties;
- members of supreme courts, of constitutional courts or of other high-level judicial bodies, the decisions of which are not subject to further appeal, except in exceptional circumstances;
- members of courts of auditors or of the boards of central banks;
- ambassadors, chargés d'affaires and high-ranking officers in the armed forces;
- members of the administrative, management or supervisory bodies of state-owned enterprises;
- directors, deputy directors and members of the board or equivalent function of an international organisation.

No public function referred to in points (a) to (h) shall be understood as covering middle-ranking or more junior officials.[85]

Due to heightened risks, MLD IV and V prescribe obliged entities to carry out an enhanced due diligence procedure (described below). Moreover, those entities are required to

(a) have in place appropriate risk management systems, including risk-based procedures, to determine whether the customer or the beneficial owner of the customer is a politically exposed person;
(b) apply the following measures in cases of business relationships with politically exposed persons:
    (i) obtain senior management approval for establishing or continuing business relationships with such persons;
    (ii) take adequate measures to establish the source of wealth and source of funds that are involved in business relationships or transactions with such persons;
    (iii) conduct enhanced, ongoing monitoring of those business relationships.

The MLD V adds a new article 20a, requiring Member States to issue and keep up to date a list indicating the exact functions which qualify as prominent public functions for the purposes of the Directive. Those lists shall be sent to the Commission and may be made public. The European Commission is likewise authorised to compile such a list for PEPs on EU-level, and so are international organisations regarding their personnel.

Moreover, the Commission is empowered to assemble, based on those lists, in a single list of all prominent public functions for the purposes of point (9) of article 3. That single list shall be made public. However, we were not able to find such a list.

[84] FATF Guidance, "Politically exposed persons (Recommendations 12 and 22)", para. 1, available at http://www.fatf-gafi.org/media/fatf/documents/recommendations/guidance-pep-rec12-22.pdf.
[85] Article 3(9) of Directive (EU) 2015/849.

3.3.3 Obligations

The MLD 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.

3.3.3.1 Due diligence

In order to perform due diligence (also known as KYC – know your client procedure), the obliged entities must be able to identify the holders of bank accounts.

Both MLD IV and MLD V prohibit the keeping of anonymous accounts. More specifically, MLD IV requires credit institutions and financial institutions from keeping anonymous accounts or anonymous passbooks. The owners and beneficiaries of existing anonymous accounts or anonymous passbooks must be subject to customer due diligence measures as soon as possible and in any event before such accounts or passbooks are used in any way.[86]

The MLD V extends the rule to apply to anonymous accounts, anonymous passbooks or anonymous safe-deposit boxes, which must then be subject to customer due diligence measures no later than 10 January 2019 and in any event before such accounts, passbooks or deposit boxes are used in any way.[87]

Due diligence must be carried out at least in the following circumstances:

- when establishing a business relationship;
- when carrying out an occasional transaction that:
    - amounts to EUR 15 000 or more, whether that transaction is carried out in a single operation or in several operations which appear to be linked; or
    - constitutes a transfer of funds, as defined in point (9) of article 3 of Regulation (EU) 2015/847 of the European Parliament and of the Council (30), exceeding EUR 1 000;
- in the case of persons trading in goods, when carrying out occasional transactions in cash amounting to EUR 10 000 or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked;
- for providers of gambling services, upon the collection of winnings, the wagering of a stake, or both, when carrying out transactions amounting to EUR 2 000 or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked;
- when there is a suspicion of money laundering or terrorist financing, regardless of any derogation, exemption or threshold;
- when there are doubts about the veracity or adequacy of previously obtained customer identification data.

Derogations are possible if appropriate mitigation measures are taken, such as having a good monitoring system in place to detect unusual or suspicious payment patterns, as per article 12. Pre-paid cards must not exceed EUR 150 (in the MLD IV: EUR 250) to be exempt from the due diligence requirement. Likewise, due diligence is triggered by cash redemptions or withdrawals and remote payments above EUR 50.

What does due diligence entail? According to article 13, it must comprise:

[86] Article 10 of Directive (EU) 2015/849.
[87] Article 10 of Directive (EU) 2018/843.

- identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from a reliable and independent source;
    - in the MLD V, this is replaced by:
    - identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from a reliable and independent source, including, where available, electronic identification means, relevant trust services as set out in Regulation (EU) No 910/2014 of the European Parliament and of the Council (*4) or any other secure,
- identifying the beneficial owner and taking reasonable measures to verify that person's identity so that the obliged entity is satisfied that it knows who the beneficial owner is, including, as regards legal persons, trusts, companies, foundations and similar legal arrangements, taking reasonable measures to understand the ownership and control structure of the customer. The MLD V also requires that, if the beneficial owner identified is the senior managing official, obliged entities must take the necessary reasonable measures to verify the identity of the natural person who holds the position of senior managing official and shall keep records of the actions taken as well as any difficulties encountered during the verification process;
- assessing and, as appropriate, obtaining information on the purpose and intended nature of the business relationship;
- conducting ongoing monitoring of the business relationship including scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the obliged entity's knowledge of the customer, the business and risk profile, including where necessary the source of funds and ensuring that the documents, data or information held are kept up-to-date.

Obliged entities must apply each of the customer due diligence requirements. However, they may determine the extent of such measures on a risk-sensitive basis. At least the variables set out in Annex I must be taken into account when assessing the risks of money laundering and terrorist financing: (i) the purpose of an account or relationship; (ii) the level of assets to be deposited by a customer or the size of transactions undertaken; (iii) the regularity or duration of the business relationship.

The obliged entities are able to demonstrate to competent authorities or self-regulatory bodies that the measures are appropriate in view of the risks of money laundering and terrorist financing that have been identified.

Due diligence necessarily entails the verification of the identity (article 14(1)). The verification of the identity of the customer and the beneficial owner must take place before the establishment of a business relationship or the carrying out of the transaction. MLD V adds the following obligation – verification must likewise be carried out "whenever entering into a new business relationship with a corporate or other legal entity, or a trust or a legal arrangement having a structure or functions similar to trusts ("similar legal arrangement") which are subject to the registration of beneficial ownership information."

3.3.3.2 Simplified customer due diligence

According to article 15(1), Member States may allow simplified due diligence for identified areas of lower risk (art. 15(1)). This is possible only if lower degree of risk is effectively established, based on factors of potentially lower risk situations in Annex II. These are:

(1) Customer risk factors, e.g. public companies listed on stock exchange, public administrations or enterprises, "residents of geographical areas of lower risk".
(2) Product, service, transaction or delivery channel risk factors: life insurance policies with low premium; products with purse limits …
(3) Geographical risk factors: EU Member States or third countries with effective anti-money laundering (AML)/combating the financing of terrorism (CFT) systems, …

Nevertheless, obliged entities are obliged to carry out sufficient monitoring of the transactions and business relationships to enable the detection of unusual or suspicious transactions.

Typically, occasional low-value transactions, such as buying gifts from Amazon, would require only simplified due diligence procedure.

3.3.3.3 Enhanced customer due diligence

In some instances, the transactions or parties involved may carry a higher risk. According to article 18, this entails situation when natural or legal entities established in the third countries identified by the Commission as high-risk third countries are involved, or higher risk is identified by the Member States or obliged entities. For example, when dealing with politically exposed persons (PEPs).

Obviously the digital coin use-case does not target being used in high-risk situations. Nevertheless, its eventual end-users are encouraged to take appropriate measures and perform risk assessment in order to comply with due diligence requirements.

3.3.4 Reporting obligations

As we already explained in D3.2, 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.[88] 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.[89] The obliged entities shall also not tip-off the customer or other third parties about the fact that information is disclosed.[90]

MLD V is said to go further than MLD IV in its reporting obligations. More specifically, it gives FIU a mandate to obtain the addresses and identities of owners of virtual currency – and so push back against the anonymity associated with the use of cryptocurrency.[91]

Alongside the due diligence requirements, reporting obligations constitute a wide-ranging exercise in data retention, which has implications for human rights and privacy. More on those in the next section.

3.3.5 Relationship with the GDPR

Recital 43 calls for attention to data protection and privacy rights of clients. More specifically, it encourages the alignment of the anti-money-laundering regulation under the revised FATF

[88] Article 33 of Directive (EU) 2015/849.
[89] Article 37 of Directive (EU) 2015/849.
[90] Article 39 of Directive (EU) 2015/849.
[91] Comply Advantage, "5AMLD – 5th EU Anti-Money Laundering Directive: What You Need to Know", https://complyadvantage.com/blog/5mld-fifth-anti-money-laundering-directive/.

Recommendations to be carried out in full compliance with Union law, in particular data protection law and the protection of fundamental rights as enshrined in the Charter.

Further, the recital specifies that implementation of the MLDs can involve the **collection, analysis, storage and sharing of data**. Such processing of personal data should be permitted, while fully respecting fundamental rights, **only for the purposes of preventing money laundering and terrorist financing**, and for the activities required such as carrying out **customer due diligence, ongoing monitoring, investigation and reporting** of unusual and suspicious transactions, identification of the beneficial owner of a legal person or legal arrangement, identification of a politically exposed person, sharing of information by competent authorities and sharing of information by credit institutions and financial institutions and other obliged entities.

The **collection and subsequent processing** of personal data by obliged entities should be limited to what is necessary for the purpose of complying with the requirements of the MLDs and personal data should not be further processed in a way that is incompatible with that purpose. In particular, further processing of personal data for commercial purposes should be strictly prohibited.

The relationship between data protection instruments, especially the GDPR, and MLDs, is therefore subject to both pieces of legislation. While the MLDs apply to the "broader" matter of preventing money laundering, the GDPR lays out more specific rules for processing personal data in this context. Therefore, we can reasonably assume that MLDs serve as *legi generali*, and the GDPR as *lex specialis*, and apply the rule of "*lex specialis derogate legi generalis*". In other words: the obligations laid out in MLDs apply unless the GDPR contains a more specific rule.

Specific binding rules are laid down in Part V (Data protection, record retention and statistical data), articles 40-44.

Art. 40 requires obliged entities to keep the following documents and information for *up to five years*:

(a) in the case of customer due diligence, a copy of the documents and information which are necessary to comply with the customer due diligence requirements laid down in Chapter II, for a period of five years after the end of the business relationship with their customer or after the date of an occasional transaction;

(b) the supporting evidence and records of transactions, consisting of the original documents or copies admissible in judicial proceedings under the applicable national law, which are necessary to identify transactions, for a period of five years after the end of a business relationship with their customer or after the date of an occasional transaction.

Point a is amended in the MLD V by:

(a) in the case of customer due diligence, a copy of the documents and information which are necessary to comply with the customer due diligence requirements laid down in Chapter II, including, where available, information obtained through electronic identification means, relevant trust services as set out in Regulation (EU) No 910/2014 or any other secure, remote or electronic, identification process regulated, recognised, approved or accepted by the relevant national authorities, for a period of five years after the end of the business relationship with their customer or after the date of an occasional transaction.

Personal data must be deleted after the expiry of this period, unless national law authorizes further storage. Such law can only be based on thorough assessment of the necessity and proportionality of such

further retention and if it is justified as necessary for the prevention, detection or investigation of money laundering or terrorist financing. In any case, the additional storage period may not exceed five more years.

If criminal proceedings are instituted, the retention of such information or documents for a further period of five years where the necessity and proportionality of such further retention has been established for the prevention, detection, investigation or prosecution of suspected money laundering or terrorist financing may be allowed or required by national law.

According to art. 41, data protection under the MLDs is wholly governed by the GDPR (or, in the case of European supervisory authorities (ESAs), the relevant Regulation (EU) 2018/1725). In the second paragraph, the *purpose limitation principle* is stressed:

> Personal data shall be processed by obliged entities on the basis of this Directive only for the *purposes of the prevention of money laundering and terrorist financing* as referred to in article 1 and *shall not be further processed in a way that is incompatible with those purposes*. The processing of personal data on the basis of this Directive for any other purposes, such as commercial purposes, shall be prohibited.

This means that obliged entities may not sell customer data for profit. Nor may third parties carrying out due diligence on their behalf, do so. Given how much insight can be gleaned from payment data, this is a very important provision. Moreover, it assuages some proportionality concerns, as discussed in this document.[92]

Moreover, customers must be provided with an information notice pursuant to now-articles 13 and 14 of the GDPR. The right to access under its article 15 may be restricted in order to

(a) enable the obliged entity or competent national authority to fulfil its tasks properly for the purposes of this Directive; or
(b) avoid obstructing official or legal inquiries, analyses, investigations or procedures for the purposes of this Directive and to ensure that the prevention, investigation and detection of money laundering and terrorist financing is not jeopardised.[93]

Under new article 43, the processing of personal data on the basis of the MLD V for the purposes of the prevention of money laundering and terrorist financing as referred to in article 1 shall be considered to be a *matter of public interest* under the GDPR. This means that complying with MLD's provisions is valid legal grounds under article 6(1)(e) of the GDPR.

3.3.5.1 Anti-money laundering, human rights and proportionality

The MLDs involve private sector (financial sector and other covered entities) in the prevention, detection, investigation and prosecution of crime. The information collected for these goals is obtained by monitoring the customer relationship and by reporting to the FIUs, which – considering the broad personal and material scope of the MLDs – can lead to collecting a large amount of data based only on an individual's transaction history. This "allows an intimate insight into that person's daily life and habits, especially if it is unpurged of unsuspicious transactions. The transaction history will contain information on the customer's wages and where he is employed, or if he receives social benefits. Rent

[92] See this interesting MIT experiment: https://news.mit.edu/2015/identify-from-credit-card-metadata-0129. Based on only four datasets from credit card metadata, 90% of individuals in this dataset were identified.
[93] Art. 41(4) of MLD IV/V.

or mortgages are included in the transaction history. The records may show when and where the person does his grocery shopping." Moreover – it may enable insight into more sensitive areas of the individual's life and habits, such as health status, sexual preferences, political orientation and so on. Under art. 9 of the GDPR, these are special categories of data and should not be processed at all. To an extent, these surveillance capabilities are mitigated by the risk-assessment approach, as described above. Nevertheless, concerns have been raised under the *proportionality criterion*, established by the CJEU in its Digital Rights Ireland case. Namely, the Directive is said to treat every customer and every transaction as potentially suspicious, despite the legitimate goal of fighting two specific crimes – money laundering and terrorist financing. This has implications for privacy, transparency, as well as the right to fair trial and presumption of innocence.[94]

3.4 Data protection principles and requirements in the digital coin scenario

Personal data are likely to be processed by post-project implementation of the FENTEC encryption and use-case. Both consumers and businesses can be among potential customers, and in each case, there may well be a data subject (employee, consumer, individual payee…) involved in the process. Hence, we discuss the interaction between GDPR, PSD2 and MLD IV/V, its relevance and give some general high-level guidelines on the implementation process.

3.4.1 Specifics of digital currency use-case

In the FENTEC use-case, functional encryption will be used to "improve citizen privacy" – as we have already described, in GDPR terms encryption is both a security measure and a pseudonymising tool. This means that it will mask and/or secure data to certain third parties who do not possess the relevant keys. In a scenario, where ensuring confidentiality is key, the division of decryption keys may have important implications for customer due diligence/know-your-customer processes. Moreover, the designation of use of digital coins with only specific merchants for specific purposes prescribed *ex ante*, may function as a kind of limitation on access to data.

3.4.2 The General Data Protection Regulation (GDPR)

Applicability of both GDPR and PSD2: personal data and sensitive payment data

GDPR applies to processing of personal data, defined in art. 4(1) as any information relating to an identified or identifiable natural person ('data subject'). This definition is important for the scope of application: if data processed do not fall into the broad category of personal data, then the legal regime of the GDPR will not apply.

On the other hand, the PSD2 mentions sensitive payment data: these are data, including personalised security credentials, which can be used to carry out fraud. These have consequences for authorisation processes (art. 5 of the PSD2) and access to data for third parties (arts. 66 and 67), but not the scope as

[94] Milaj, J., Kaiser, C., "Retention of data in the new Anti-money Laundering Directive—'need to know' versus 'nice to know'", International Data Privacy Law, Vol. 7, Issue 2, May 2017, 115–125, https://doi.org/10.1093/idpl/ipx002.

such. The interaction between the two terms is not well researched: Deloitte[95] points out that the lack of clarity may bring unnecessary regulatory risks to banks, since the duty to distinguish between the different types of data is largely left to them as data controllers and bound entities under the PSD2.

Functional encryption can help: ***appropriate use of algorithm and division of encryption keys*** may contribute to security of personalised credentials, as required in arts. 66, 67 and 69, and more specifically under the Regulatory Technical Standards (RTS).

Data quality principles

The use of functional encryption in the digital coin scenario may have an impact on the implementation of data protection principles.

1. **Lawfulness, fairness and transparency**. This principle is threefold – most importantly, it pertains to trust and empowerment of the individual using digital services, since properly established transparency procedures facilitate the exercise of rights, including remedy and challenge of a decision. Information requirements include disclosing basic security measures taken by the controller.[96] Transparency includes, but is not limited to ensuring adequate information is given to the user. Therefore, following articles 13 and 14 of the GDPR, as well as pre-contractual information obligations contained in art. 56-60 of the PSD2, ***once implemented in a post-project scenario, the digital coin adopters should disclose relevant information pursuant to GDPR and PSD2 to the service users***. ***Relevant legal grounds*** must exist in order for processing to be legitimate; this is covered in the next section on art. 6.
2. **Purpose limitation**: data may only be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. In the digital coin scenario, customer data can be used for anti-money laundering purposes as defined in the MLDs, and ***for other purposes only to the extent relevant legal grounds exist*** (for example, user consent, necessity for performance of a contract etc.).
3. **Data minimisation**: the data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. Functional encryption has a potentially high impact on this principle: depending on the distribution of keys, certain actors may or may not access personal data. ***Due caution must be given to distribution of keys*** in order to enable data minimisation principle.
4. **Accuracy of data**: implementation of this principle will be best achieved in a post-project setting.
5. **Storage limitation**: MLDs restrict the limit for data storage for ***up to five years after the end of a business relationship***, unless limited exceptions for longer storage apply.
6. **Integrity and confidentiality**: encryption in a digital coin scenario may be considered as an appropriate technical measure to ensure appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

[95] Deloitte Luxembourg: PSD2 and GDPR – friends or foes? https://www2.deloitte.com/lu/en/pages/banking-and-securities/articles/psd2-gdpr-friends-or-foes.html.

[96] Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, adopted on 29 November 2017, last revised and adopted on 11 April 2018, WP260 rev.01.

Legal grounds for data processing

Art. 6 of the GDPR provides for different legal grounds for data processing. In the digital coin setting, based on legal framework examined, three possible grounds emerge:

1. **Consent of the data subject**

Very often, users of payment apps will consent to the processing of their data, when they agree with the service's privacy policy and/or terms or conditions. Nevertheless, some obligations must be respected when asking for consent:[97]

- Consent must be freely given, specific, informed and unambiguous indication of the data subject's wishes (art. 4(11) of the GDPR)
- The controller must keep record of the data subject's given consent
- Consent may be revoked at any time without consequences

PSD2 and GDPR at times require explicit consent, or "normal" consent. The differences were discussed in section 3.2.3, including the fact that the PSD2's notion of explicit consent may refer to other legal grounds outside consent.

2. **Necessary to carry out a contract**

Data processing is lawful if it is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract. This may be the case when a third party is involved in the execution of a payment service, for example as a payment services initiation provider, or an account information service provider.

It is important to note that assessing what is 'necessary' involves a combined, fact-based assessment of the processing "for the objective pursued and of whether it is less intrusive compared to other options for achieving the same goal". If there is an option that enables the fulfilling of the contract without intrusive processing of personal data, then such processing cannot be considered necessary. In such cases, another legal grounds must be sought.[98]

3. **Task in the public interest**

Sometimes, it is not possible to ask for consent without jeopardising the objectives. In art. 39, MLDs specify the prohibition of disclosure to customers that (or which) information is being reported to FIUs or that a money laundering or terrorist financing analysis is being, or may be, carried out.

The new article 43 of the MLD V instead provides that carrying out procedures pursuant to it is considered to be a task in the public interest. These are valid legal grounds under art. 6(1)(e), providing that the necessity criterion is met.

Due diligence in choosing processors, sub-contractors and third party providers

Financial institutions often employ third parties to perform certain tasks in the execution of payment services or to perform customer due diligence on their behalf. While this is common business practice,

[97] Article 29 Working Party, Guidelines on consent under Regulation 2016/679, adopted on 28 November 2017, last revised and adopted on 10 April 2018.
[98] European Data Protection Board, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, Version 2.08, October 2019.

certain data protection standards must nevertheless be respected in the choice and in the relationship with the third party/sub-contractor.

Under the GDPR, the entity, which carries out the processing operation on behalf of the controller, is called a processor. It can only be appointed if it meets certain criteria. According to article 28(1) of the GDPR, the controller must use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject..

Therefore, data controllers – PSPs and entities bound by the MLDs, adopting the digital coin scenario, should exercise care and perform due diligence on their envisioned processors before entering into a data processing activity.

The controller and the processor can regulate their relationship by concluding a contract to that end. This is sometimes referred to as 'processor terms'. GDPR only sets out their minimum content. Processor terms can be based, wholly or partly, on standard contractual clauses, which the Commission or another supervisory authority will adopt.[99] They must be in writing, including in electronic form.[100]

Data subjects rights

Two of the data subjects rights are especially relevant for the digital coin scenario. First, we will talk about the **right to portability in open banking/open finance**; secondly, about the **right to access information held by the banks in the context of KYC/due diligence**.

1. Open finance/open banking is a relatively new technique to bypass banks and other financial institutions. It enables consumers to easily transfer their accounts and data from one provider to another, including to banks which are completely digital.[101] Technologies such as biometric software, government ID document readers, and identity and access management (IAM) solutions all support the secure transition from traditional to open banking interactions. [102] On the legal side, this shift is driven by the legislative cocktail of PSD2, MIFIR/MIFID2[103] and the GDPR. In the PSD2, the legal regime of access to data has already been described – let us reiterate that non-traditional providers of payment services may, under certain conditions, access the customer data held by banks. The GDPR's right to data portability, contained in its art. 20, is the mirror right from the consumer's point of view:

The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided.

This right applies if the processing is based on consent pursuant to point (a) of article 6(1) or point (a) of article 9(2) or on a contract pursuant to point (b) of article 6(1); and the processing is carried out by

[99] Article 28, (6-8) of the GDPR.
[100] Article 28, (9) of the GDPR.
[101] Consumers will benefit most from open banking, says plum. (2018, Jan 12). *Banking Newslink.*
[102] OPEN BANKING: PUTTING CONSUMERS IN THE DRIVER'S SEAT. (2019). *Banker, Middle East,*
[103]MiFID II/MiFIR became applicable on 3 January 2018. This new legislative framework has strengthened investor protection and improved the functioning of financial markets making them more efficient, resilient and transparent. See: Markets in Financial Instruments (MiFID II) - Directive 2014/65/EU; Markets in Financial Instruments (MiFIR) - Regulation (EU) No 600/2014.

automated means. This is often the case in payment services. The data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible; otherwise, the data subject receives the personal data about themselves and takes care that they are transferred to another provider.

2. Right to access and the KYC/customer due diligence procedure

Under the GDPR the data subject has the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and certain information about the processing. This includes giving a copy of the personal data to the data subject; however, the right to obtain a copy shall not adversely affect the rights and freedoms of others.[104] This presents **the first possible restriction** of the right – if fighting money laundering and terrorism financing falls under the umbrella of p**rotection of the rights and freedoms of others**, then the reception of personal data under this article may not jeopardise these goals.

Another restriction can be found in art. 23, which allows for **restricting data subjects rights** under certain conditions:

- The restriction must be laid down in legislation on EU or national level,
- The restriction can refer to articles 12 to 22 and article 34, as well as article 5 in so far as its provisions correspond to the rights and obligations provided for in articles 12 to 22,
- The restriction must respect the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard important interests, among them the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. This provision may well apply to fighting money laundering.

A third restriction can be found **in the MLDs** – the right to access may be restricted in order to

(a) enable the obliged entity or competent national authority to fulfil its tasks properly for the purposes of this Directive; or
(b) avoid obstructing official or legal inquiries, analyses, investigations or procedures for the purposes of this Directive and to ensure that the prevention, investigation and detection of money laundering and terrorist financing is not jeopardised.

Therefore, we can conclude that access to information held by banks for KYC purposes is very limited thanks to legal restrictions. As far as FENTEC use-caseis concerned, those restrictions can be managed by appropriate division of decryption keys among the actors: ***following the principles of proportionality and necessity, only the actors who cannot access relevant information without obtaining the decryption key, can ask access to such a key***.

Data protection and data security by design

Data controllers – most likely future FENTEC digital coin adopters, such as PSPs – are required by the GDPR to lay down appropriate organisational and technical measures in order to ensure and demonstrate compliance (arts. 5(2) and 24), data protection by design and by default (art. 25) and security by design (art. 32). We have already described the relevance of functional encryption to technical measures adopted to these ends in Sections 2.3.2, 2.3.3 and 2.3.4. Of course other measures should be used as

[104] Art. 15 (1), 15 (3), 15 (4) of the GDPR.

well, such as access controls, no default passwords, data minimisation measures, etc.; measures described in those sections fully apply to this use-case. Regarding organisational measures, it must be noted that due to the financial sector often being targeted by cyber-attacks, training personnel and implementing company-wide cyber-security practices is necessary. In fact, banking sector and financial markets infrastructures operators are also subject to the Networks and Information Systems Security (NIS) Directive,[105] which imposes some additional obligations in terms of reporting and technical and organisational measures.

Appointment of a data protection officer (DPO)

The controller and the processor shall designate a data protection officer in the following three cases:

- the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
- the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or
- the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to article 9 and personal data relating to criminal convictions and offences referred to in article 10.

Procedures, such as preventing money laundering and terrorism financing, undoubtedly fall under the second alinea, according to the Article 29 Working Party's Opinion.[106] Therefore, ***we suggest that FENTEC digital coin adopters appoint a DPO***, taking into account the legal framework described below.

An appropriate DPO is one with a good level of expertise, which depends on the sensitivity and amount of the data processed and the complexity of the processing operation. He or she must have expert knowledge of EU data protection laws, as well as the basic tenets of the processing operation. He or she may be a staff member of the controller or processor, or fulfil the tasks on the basis of a service contract.

While a DPO monitors the compliance, the overall responsibility to comply with the GDPR remains with the data controller, or its processor, according to the accountability principle.[107] A DPO is autonomous in carrying out their tasks, but that does not mean they have decision-making powers beyond article 39, i.e. giving advice on data processing, monitoring compliance with the GDPR, advising on the implementation of the DPIA, cooperating with the supervisory authority, and act as the main contact point for prior consultation under article 36.

The contact details of the DPO must be published and notified to the supervisory authority[108] in order to ensure that the DPO may be contacted confidentially and discreetly by both data subjects and the authorities. The Article 29 Working Party opinion also recommends informing the workforce about the DPO's name and contact details as a good practice.[109]

[105] 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.
[106] Article 29 Working Party, Guidelines on Data Protection Officers ('DPOs'), adopted on 13 December 2016, last revised and adopted on 5 April 2017, p. 21.
[107] Article 5, (2) of the GDPR.
[108] Article 37, (7) of the GDPR.
[109] Article 29 Working Party, Guidelines on data protection officers (DPO), WP243, 13/12/2016, p. 13.

Adoption of a data protection impact assessment (DPIA)

A DPIA must be adopted for situations which comprise "a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person". It is possible that KYC procedures may well fall under this provision. Banks often have in place automated systems, which scrutinise every transaction made by the customer and build a risk profile accordingly. The Article 29 Working Party specifically suggest that screening customers against a credit reference database or against an anti-money laundering and counter-terrorist financing (AML/CTF) or fraud database by financial institutions could be considered as evaluation/scoring, and therefore also fall under the "high risk" criterion.[110] ***A DPIA is therefore necessary for adopters of FENTEC digital coin.***

[110] Article 29 Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, WP 248.

4 Video surveillance scenario

In this use-case functional encryption is applied to video surveillance infrastructure in order to enable gateway systems to detect motion on the stream, thus allowing the gateway to make decisions based on the presence or absence of motion. This system structure enables local decision-making at the gateway level while preserving the privacy and security of processed data.

This chapter examines the applicable legal requirements that can be derived from legislation in the field of privacy and data protection. The requirements applicable to video surveillance mainly stem from national legislation and relate to the end-use of video surveillance technology. As an example, the Belgian Camera Act will be discussed.

4.1 The General Data Protection Regulation (GDPR)

The GDPR lays down a set of legal requirements to ensure the proper processing of personal data by data controllers and processors. While many of these requirements are general in nature and apply to all use-cases in FENTEC, some of them may be particularly relevant for the video surveillance use-case. Following the 'data protection by design' principle, these requirements should be taken into account from the outset.[111] Consequently, the responsibility to adhere to the principles of the GDPR falls upon the eventual data controllers and/or processors (i.e. entities that make use of video surveillance technologies), as well as the developers and designers of technologies.

The use of smart cameras for video surveillance purposes generally gives rise to more privacy and data protection risks. The video surveillance use-case in FENTEC, however, makes use of functional encryption in order to minimize the amount of transferred unencrypted data. This allows for more secure data processing in general, to the benefit of user privacy. Since the GDPR takes on a risk-based approach, the increased security aids in complying with some of the legal requirements that may apply.

4.1.1 Lawfulness of processing (art. 6 GDPR)

The requirement of 'lawfulness' is a data protection principle[112] which makes clear that the processing of personal data must be based on, and limited to, a legal ground. Due to the differences between use-cases, and therefore also in the application of legal grounds, it is relevant to include lawfulness under this section. The lawfulness requirement creates an obligation for the data controller to rely on one of the six legal grounds provided in article 6 of the GDPR. In principle, every legal ground found in article 6 is valid in the case of video surveillance, however, the legal grounds of '*compliance with a legal obligation*'[113], '*legitimate interest*'[114], and '*a task carried out in the public interest*'[115] will be the most suitable options.

[111] Article 25 of the GDPR.
[112] Article 5, 1, (a) of the GDPR.
[113] Article 6, 1, (c) of the GDPR.
[114] Article 6, 1, (f) of the GDPR.
[115] Article 6, 1, (e) of the GDPR.

4.1.1.1 Compliance with a legal obligation (art. 6, (c) GDPR)

In many cases the processing of personal data by using video surveillance is lawful if it is necessary for compliance with a legal obligation to which the controller is subject. This applies to controllers from both the private and public sector.[116] It is important to note that the legal obligation must be laid down by Union or Member State law to which the controller is subject. Member States are allowed to maintain or introduce more specific provisions to adapt the application of the GDPR in relation to this legal basis. They may do so by laying down specific requirements and measures to ensure lawful and fair processing of personal data.[117] The Union or Member State law which provides for the legal basis must be sufficiently clear and shall determine the purpose of processing. It further may specify the general conditions of processing, the types of data, the data subjects concerned, storage periods, etc. This law must also meet an objective of public interest and must be proportionate to the aim pursued.[118] A legal obligation for video surveillance may exist for the purpose of public safety and security, such as the use of body cameras by law enforcement authorities or the placement of surveillance cameras in high-risk areas. It must also be noted that the use of video surveillance may not be voluntary and that the controller must not have any choice in fulfilling the legal obligation.[119]

4.1.1.2 The legitimate interests pursued by the data controller or third party (art. 6, (f) GDPR)

The processing of personal data through the use of video surveillance is lawful if it meets the conditions of article 6, (f) of the GDPR. First of all, there must exist a legitimate interest pursued by the controller or a third party. This legitimate interest can be legal, economic, or non-material in nature, and must relate to a real and present issue.[120] An example of a legitimate interest could be the protection against vandalism, theft, or burglary, but only if it can be proven that there exists a real situation of distress to warrant the use of video surveillance (f.e. by providing evidence of previous incidents, crime statistics of the specific area, the special nature of the business, etc.).[121]

Secondly, the processing of personal data should be limited to what is adequate, relevant, and necessary for the specified purposes. The requirement of 'necessity' is explicitly mentioned in article 6, 1, (f) of the GDPR, but is also better known as the '*data minimisation'* principle laid down in article 5, 1, (c) of the GDPR. Following this requirement, video surveillance measures should only be implemented if other less intrusive measures cannot reasonably fulfill the purposes of processing (f.e. security personnel, fencing, security locks, etc.). Necessity also applies to the specific method of surveillance, such as the use of black box solutions or real-time monitoring. The data controller should make an assessment of the particular situation at hand.[122]

Lastly, in order to rely on the legal ground of legitimate interest, it is mandatory to balance the interests of the parties involved. The data controller can only rely on this legal ground if its legitimate interests are not overridden by the interests or fundamental rights and freedoms of the data subject.[123] For this

[116] The European Union Agency for Fundamental Rights, the Council of Europe, and the European Data Protection Supervisor, " Handbook on European data protection law", 2018, 151.
[117] Article 6, 2 of the GDPR.
[118] Article 6, 3 of the GDPR.
[119] Article 29 Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under article 7 of Directive 95/46/EC, adopted on 9 April 2014, 19.
[120] Ibid., 24.
[121] European Data Protection Board, "Guidelines 3/2019 on processing of personal data through video devices", 10 July 2019, 8.
[122] Ibid., 8-9.
[123] Article 6, 1, (f) of the GDPR.

reason, the controller must assess the effects and possible negative consequences of video surveillance on these interests or fundamental rights and freedoms. This balancing exercise is done on a case-by-case basis, taking into account the specific factors of a particular situation.[124] The intensity of intervention (f.e. the type of collected data, the number of data subjects, the scope of processing, the particular situation and interests, alternative options, etc.) is considered the most important factor in this balancing exercise.[125] Recital 47 of the GDPR also tells us that the reasonable expectations of the data subject at the time and in the context of the collection of personal data must be taken into account.[126] This reasonable expectation should be determined from the point of view of an objective third party and whether or not this third party could reasonably expect to be monitored in the specific situation at hand (f.e. a data subject would not reasonably expect to be monitored in sanitary facilities or in an examination room). The presence of video surveillance signs, as mandated by national legislation in some countries, does not change this reasonable expectation from the point of view on an objective third party.[127]

The legal ground of legitimate interest cannot be invoked by public authorities in the performance of their tasks.[128]

4.1.1.3 A task carried out in the public interest or in the exercise of official authority vested in the controller (art. 6, (e) GDPR)

Other viable legal bases for video surveillance are (1) the reliance on a task carried out in the public interest or (2) in the exercise of official authority vested in the controller. Processing based on this legal ground should be laid down by Union law or Member State law to which the controller is subject. The implementing legislation may specify the conditions and modalities for video surveillance (f.e. purposes of processing, general conditions, types of data, storage periods, processing procedures, etc.), in accordance with the GDPR. It must meet an objective of public interest and be proportionate in nature.[129] As with legitimate interest, the video surveillance measures must be necessary for the performance of the public task in question.[130] An example would be the use of video surveillance for the purpose of ensuring the safety and security of large public events.

4.1.2 Special categories of data (art. 9 GDPR)

Particularly in the context of video surveillance, it should be reminded that some categories of personal data receive special handling, such as an increased level of security, due to their highly sensitive nature. More specifically, the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation is in principle prohibited.[131]

---

[124] Article 29 Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under article 7 of Directive 95/46/EC, adopted on 9 April 2014, 33.
[125] European Data Protection Board, "Guidelines 3/2019 on processing of personal data through video devices", 10 July 2019, 9.
[126] Recital 47 of the GDPR.
[127] European Data Protection Board, "Guidelines 3/2019 on processing of personal data through video devices", 10 July 2019, 9.
[128] Article 6, 1 of the GDPR.
[129] Article 6, 3 of the GDPR.
[130] Article 29 Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, adopted on 9 April 2014, 21.
[131] Article 9, 1 of the GDPR.

Exceptionally, the processing of the so-called sensitive data is allowed in specific situations provided for by article 9, 2 of the GDPR. Furthermore, one of the abovementioned legal grounds for the processing of personal data in general, as set out in article 6 of the GDPR, should always apply cumulatively with one of these specific exceptions.

The processing of special categories of personal data is allowed, for instance, when it is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, shall respect the essence of the right to data protection and shall provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.[132] In addition, as a matter of example, the processing of sensitive personal data is allowed if it is necessary to protect the vital interests of the data subject, where the data subject is physically or legally incapable of giving consent.[133] This legal ground will only be applicable in exceptional situations of emergency, for instance when a hospital monitors a patient for medical reasons and this person was brought in unconscious.[134] Finally, not every exception of article 9, 2 will be appropriate in the context of video surveillance. For example, article 9, 2, (e), which relates to the processing of personal data that are manifestly made public by the data subject, can generally not be invoked by the controller. Merely moving into range of a camera does not mean that the data subject intends to make public his/her special categories of personal data.[135]

4.1.3 Data minimisation and storage limitation (art. 5, (c) and (e) GDPR)

Personal data must always be adequate, relevant, limited, and kept in a form which permits identification of data subject for no longer than what is necessary for the purposes for which they are processed.[136] Member States may, depending on the legal basis, introduce specific storage periods for video surveillance activities.[137] In any case, the appropriate storage period will depend on the purposes of processing. For example, video surveillance may serve the purpose of preserving evidence, which warrants a longer storage period than the sole purpose of detecting vandalism. Consequently, a longer storage period requires more weight to the legitimacy of the purpose and necessity of the storage measure.[138] For example, the Belgian Camera Act lays down that the recording video footage is exclusively allowed in order to collect evidence of hindrance, crime or damages, and to track and identify offenders, disturbers of the public order, witnesses, or victims. If the footage does not contribute to these purposes, it may not be stored longer than one month.[139] It is advised to adopt clear policies for video surveillance and storage periods.

4.1.4 Transparency and information obligation (art. 12 and 13 GDPR)

The processing of personal data through video surveillance technology is, like other processing activities, subject to the transparency and information obligations of articles 12, 13, and 14 of the GDPR. In the specific case of video surveillance, the information to be provided is determined by article 13,

[132] Article 9, 1, (g) of the GDPR.
[133] Article 9, 1, (c) of the GDPR.
[134] European Data Protection Board, "Guidelines 3/2019 on processing of personal data through video devices", 10 July 2019, 14.
[135] Ibid., 15.
[136] Article 5, 1, (c) and (e) of the GDPR.
[137] Article 6, 2 of the GDPR.
[138] European Data Protection Board, "Guidelines 3/2019 on processing of personal data through video devices", 10 July 2019, 24.
[139] Article 5, (4) of the Act of 21 March 2007 regulating the installation and use of surveillance cameras.

since the personal data is collected from the data subject. These obligations entail that the data subject should be informed about the surveillance activities in a detailed and transparent manner. For video surveillance, a layered approach is often preferred, where information is provided through multiple channels (f.e. a warning sign, information sheet, website, etc.).[140]

The first layer of information should be provided by placing a warning sign. This is often done in combination with standardized icons in order to give in an easily visible, intelligible and clearly legible manner an overview of the intended processing activities.[141] The aim is to inform the data subject in such a way that he/she recognizes the circumstances of the surveillance activities before entering the area in question. The context of surveillance and which areas are under surveillance must be clear to the data subject. This warning sign, as a first channel of information, should provide the most important information (f.e. details on the purposes of processing, the legal basis, the identity of the controller, the rights of data subject, the contacts details of the DPO, etc.) and, if applicable, any special information (f.e. transfer to third parties, storage periods, etc.). It should also make a clear reference to the second layer of information, which provides more detailed information.[142]

The second layer of information, to which the first layer must clearly refer, should provide all the necessary information of article 13 in a detailed manner. This layer must be easily accessible and can be made available both digitally (f.e. a website) or non-digitally (f.e. an information sheet, a poster, etc.). It is recommended that, in case the second layer is provided digitally, there also exists a non-digital channel. In any case, the second layer of information should be accessible without entering the surveilled area.[143]

According to the requirement of transparency, all of this information must be communicated in a concise, transparent, intelligible and easily accessible form, using clear and plain language.[144] It must be noted that these transparency and information obligations are often further specified under applicable national law, which should also be taken into account.

4.1.5 Data subject rights (art. 15 – 22 GDPR)

The data subject rights provided for by the GDPR represent entitlements and claims the individual data subject has vis-à-vis the data controller. Conversely, they reflect in corresponding responsibilities and obligations of data controllers or the data processor on behalf of the controller. In light of this, one of the practical consequences of data subject rights is that the controller has to be organizationally prepared for them, for example by providing a contact point, portal, or access to information and data subject requests.

The GDPR provides both for exceptions on the exercise of certain individual data subject rights as well as a general provision of restriction similarly applicable to the exercise of all the data subject rights. Accordingly, the controller may be exempted from complying with data subject requests, under the specific conditions of article 23.

[140] Ibid., 21.
[141] Article 12, 7 of the GDPR.
[142] European Data Protection Board, "Guidelines 3/2019 on processing of personal data through video devices", 10 July 2019, 22.
[143] Ibid., 23.
[144] Article 12, 1 of the GDPR.

4.1.5.1 Right of access

The data subject has the right to obtain from the controller confirmation as to whether or not their personal data are being processed. If this is the case, the data subject also has the right to access and obtain all the information they are entitled to under article 15.[145] They may also request a copy of the data undergoing any processing.[146] However, this right to obtain a copy may not adversely affect the rights and freedoms of others.[147] Providing a copy of video surveillance footage may, in some cases, have such an effect. As a result, there exist situations where a controller should refuse the request to obtain a copy due to the identifiability of other individuals. Technical measures (f.e. editing, masking, etc.) may be implemented in order to fulfill these requests.[148]

In case of real-time monitoring, the controller will only be able to satisfy the transparency and information requirements of article 12 and 13 since no personal data is being stored or otherwise processed. If personal data is being stored or processed beyond real-time monitoring, then the right of access and information under article 15 will apply.[149]

According to article 11, 2 of the GDPR, articles 15 to 20 will not apply if the controller is able to demonstrate it is not in a position to identify the data subject, unless the data subject provides additional information enabling his/her identification.[150] This could be the case when video surveillance records a large number of individuals in a frequented area. For the purpose of exercising his/her rights, the data subject should then provide additional information, such as the timeframe he/she entered the surveilled area.

4.1.5.2 Right to rectification

The data subject has the right to the rectification of inaccurate personal data concerning her or him without undue delay.[151] This right is not as relevant in the context of video surveillance activities.

4.1.5.3 Right to erasure ("right to be forgotten")

The data subject has the right for personal data concerning him/her to be erased by the controller without undue delay provided one of the legitimate grounds for erasure is demonstrated.[152] This right cannot be exercised where it is limited by; the right of freedom of expression and information, a legal obligation, a task in the public interest or in the exercise of official authority, reasons of public interest in the area of public health, proportional archiving, research, or statistical purposes, and purposes of legal claims.[153]

[145] Article 15, 1 of the GDPR.
[146] Article 15, 3 of the GDPR; a copy of such data must be provided free of charge, but the controller may charge the data subject reasonable administrative fees for any further copies.
[147] Article 15, 4.
[148] European Data Protection Board, "Guidelines 3/2019 on processing of personal data through video devices", 10 July 2019, 19.
[149] Ibid., 18-19.
[150] Article 11, 2 of the GDPR.
[151] Article 16 of the GDPR.
[152] Grounds for erasure in article 17.1 of the GDPR: the personal data are no longer necessary in relation to the purpose for which they were collected, the data subject withdraws consent and there is no other legal ground for the processing, the data subject objects to the processing and there is no overriding legitimate grounds for processing, the personal data have been unlawfully processed, for compliance with legal obligation, the personal data have been collected in relation to the offer of information society services.
[153] Article 17, 3 of the GDPR.

In case the video footage has been made public, the controller shall take reasonable steps to inform other controllers which are processing personal data that the data subject has requested its erasure. These steps include technical measures, taking account of available technology and the cost of implementation.[154]

4.1.5.4 Right to restriction of processing

In certain situations, where there is a challenge between the data subject and the data controller, the former is entitled to the restriction of data processing for a period until the issue is resolved. Such cases are when an individual disputes data accuracy, when they object to processing (on legitimate interests), when the processing is unlawful but the individual objects to erasure and requests restriction instead and when the controller has no further need for the data but the individual requires the personal data to establish, exercise, or defend legal claims.

Restriction of data processing means the controller may store the personal data, but any further processing can only take place either with the data subject's consent or for the establishment, exercise or defense of legal claims, the protection of the rights of another natural or legal person or for reasons of important public interest of the EU or of a Member State.[155]

4.1.5.5 Right to data portability

While the data subject access gives individuals the right to require their data to be provided in a commonly used electronic form, data portability goes a step further – the data subject is entitled to ask the controller to provide information in a structured, commonly used and machine readable form so that it may be transferred to another controller. Where technically feasible, the data subject is entitled to demand that personal data is transmitted directly from one controller to another.

However, portability is narrower in scope than right to data access, as it only applies to personal data which is processed by automated means (no paper records) and which the data subject has provided to the controller and only where the basis for processing is consent and fulfilment of contract.[156]

4.1.5.6 Right to object

Every data subject has a right to object three types of processing, namely 1) the processing for direct marketing purposes, 2) the processing based on legitimate interest or because it's necessary for public interest or in the exercise of official authority and 3) the processing for scientific, historical, research or statistical purposes.

In case of the first two types of processing, the right to object should be explicitly brought to the attention of the individual at the latest during the first communication with them.

When it comes to processing in legitimate or public interest, in the event of an objection the controller must cease the processing unless she or he can demonstrate compelling legitimate grounds which override those of the data subject or that the processing is for the establishment, exercise or defense of legal claims.[157]

[154] Article 17, 2 and 19 of the GDPR.
[155] Article 18 of the GDPR.
[156] Article 20 of the GDPR.
[157] Article 21 of the GDPR.

For video surveillance activities, the controller must be able to stop the processing of personal data when requested or, in case of a restricted area, must receive approval from the data subject prior to entering.[158]

4.1.5.7 Restriction of rights

The scope of application of data subject rights may be restricted by EU or Member State law on the basis of a legislative measure.[159] The general condition for restriction is that it respects the essence of the fundamental rights and freedoms, and is necessary and proportionate for the achievement of one of the enumerated legitimate goals, including inter alia national security, defense, public security, investigation, prosecution and sanctioning of criminal offences, monitoring or regulatory function connected to the exercise of official authority and other important objectives of general public interest.

4.1.6 Appropriate technical and organizational measures (art. 5, 24, 25, and 32 GDPR)

In the context of security[160], the application and implementation of the data protection principles[161], and safeguarding the rights and freedoms of the data subject, controllers are required to implement appropriate technical and organizational measures.[162] These measures must be, on the basis of data protection by design and by default principle, implemented at the time of the determination of the means of processing and at the time of processing itself.[163] In general, organizational measures relate to enforcing the proper management frameworks, procedures, and policies (f.e. a DPIA, access policies, training program, transfer policies, incident management, etc.), while technical measures involve the inclusion of requirements in the design and specification of the system architecture (f.e. cybersecurity measures, physical protection, encryption, access rights, authentication and authorization measures, system restoration, etc.). The controller should also aim for the implementation of privacy-friendly technologies and measures, but only to the extent that they are necessary (f.e. integrated scrambling and editing software, limited movement and zoom capabilities, limited analytics).[164]

4.1.7 Data protection impact assessment (art. 35 GDPR)

As explained in Section 2.3.5, a DPIA must be conducted when a type of processing is likely to result in a high risk to the rights and freedoms of natural persons. In any case, a DPIA is mandatory in three situations:

1. a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
2. processing on a large scale of special categories of data referred to in article 9(1), or of personal data relating to criminal convictions and offences referred to in article 10; or

[158] European Data Protection Board, "Guidelines 3/2019 on processing of personal data through video devices", 10 July 2019, 21.
[159] Article 23, 1 GDPR.
[160] Article 32 of the GDPR.
[161] Article 5 and 25, 1 of the GDPR.
[162] Article 24 of the GDPR.
[163] Article 25, 1 of the GDPR.
[164] European Data Protection Board, "Guidelines 3/2019 on processing of personal data through video devices", 10 July 2019, 26-28.

3. a systematic monitoring of a publicly accessible area on a large scale.[165]

In the context of the research activities in the video surveillance use-case, conducting a DPIA will not be necessary, since none of the abovementioned situations apply. However, for the end-use of video surveillance technology, it will be mandatory to conduct a DPIA when systematically monitoring a publicly accessible area or processing special categories of data on a large scale, which is often the case in a surveillance scenario, especially by a public authority. The fulfilment of this requirement is an obligation for the controller and will have to be assessed on a case-by-case basis. The supervisory authority of each Member State must also publish a list of processing activities that require a DPIA.[166] An example of such a list is the one published by the Belgian DPA in January, 2019. One of the identified processing activities that requires a DPIA is the *"wide-scale processing of data generated by means of devices with sensors that send data through the internet or another medium ('internet of things' applications, such as; smart televisions, smart appliances, smart meters, etc.) and the processing of which serve to analyze or predict the economic situation, health, personal preferences or interests, reliability or behavior, and location or movement of natural persons."*.[167] This situation applies when smart cameras analyse or predict the location or movement of individuals. The identified processing activities by national DPAs apply in addition to the situations laid down in article 35, 3 of the GDPR.

4.2 National legislation: the Belgian Camera law

The smart video surveillance technology developed in this use-case can be used by both public and private entities. Since the use of video surveillance is primarily subject to national legislation, an overview of the legal requirements derived from Belgian legislation will be provided as an example. These requirements apply to the end-use of the FENTEC video surveillance technology within the Belgian territory.

The revised Belgian Camera Act, applicable from the 25th of May 2018, regulates the use of surveillance cameras in specified and defined areas. Because the scope of application has already been discussed in D3.2, the analysis below will be limited to the identification of applicable legal requirements.

The subject matter of the Belgian Camera Act is divided into three chapters, namely; (1) conditions for the placement and use of fixed and temporarily fixed surveillance cameras, (2) conditions for the use of mobile surveillance cameras, and (3) common provisions. Secondly, the provisions of the Camera Act make a distinction between surveillance cameras placed in (1) non-enclosed areas, (2) publicly accessible enclosed areas, and (3) enclosed areas not accessible to the public.

[165] Article 35, (3) of the GDPR.
[166] Article 35, (4) of the GDPR.
[167] Privacy Commission, List of the types of processing operations for which a Data Protection Impact Assessment shall be required conform article 34, 4 of the GDPR (CO-A-2018-001), 16 January 2019, 3.

4.2.1 Fixed and temporarily fixed surveillance cameras

4.2.1.1 Non-enclosed areas

The decision to place one or more fixed or temporarily fixed surveillance camera in non-enclosed areas, such as a public space, is taken by the controller, which must be a public authority.[168] The decision must also be notified to the police department and requires a positive assessment of the municipal council.[169]

The Belgian Camera act also contains an obligation for the controller to keep a register with the processing activities of the surveillance cameras under its responsibility. This register must be made available to the DPA and police department on request.[170] The controller must also place a pictogram at the entrance of the non-enclosed area, in order to inform the data subject of the presence of video surveillance.[171]

In any case, the controller must make sure that the surveillance camera is not specifically aimed at an area for which the controller does not process data, unless explicit consent has been obtained from the controller of that specific area.[172]

The viewing of footage in real-time is exclusively allowed under supervision of the police department, so that the competent authorities can intervene in case of crime, damages, hindrance or disturbance of public order. The conditions to determine which persons have competence to view this real-time footage are determined by Royal Decree. The access to footage in real-time is also allowed to enable competent authorities to coordinate the security of important events that have an impact on public order and public safety, and to assess and coordinate emergency situations.[173] On the other hand, recording video footage is exclusively allowed in order to collect evidence of hindrance, crime or damages, and to track and identify offenders, disturbers of the public order, witnesses, or victims. If the footage does not contribute to these purposes, it may not be stored longer than one month. This period is extended to three months for areas that incur a special security risk, laid down in a Royal Decree.[174]

4.2.1.2 Publicly accessible enclosed areas

The obligations for the placement of fixed and temporarily fixed surveillance cameras in publicly accessible enclosed areas are generally the same as for non-enclosed areas. Some differences are, however, import to mention.

First of all, a positive assessment by the municipal council is not required for the placement of surveillance cameras in publicly accessible enclosed areas.

Secondly, similar to non-enclosed areas, the controller must ensure that the surveillance camera is not specifically aimed at an area for which the controller does not process data. When the entrance of a publicly accessible enclosed area is surveilled, opposite to a non-enclosed area or publicly accessible enclosed area, the surveillance camera must be aimed in such a way that it limits the surveillance of that area to a strict minimum.[175]

---

[168] Article 5, (1) and (2/1) of the Act of 21 March 2007 regulating the installation and use of surveillance cameras.
[169] Article 5, (2), (2/1), and (3) of the Act of 21 March 2007 regulating the installation and use of surveillance cameras.
[170] Article 5, (3) of the Act of 21 March 2007 regulating the installation and use of surveillance cameras.
[171] Ibid.
[172] Ibid.
[173] Article 5, (4) of the Act of 21 March 2007 regulating the installation and use of surveillance cameras.
[174] Ibid.
[175] Article 6, (2) of the Act of 21 March 2007 regulating the installation and use of surveillance cameras.

An important difference with non-enclosed spaces is that the controller may place, in the vicinity of the surveillance camera, a display that publicly shows the real-time video footage of the surveillance camera.[176] Additionally, the viewing of real-time video footage is exclusively allowed in order to intervene in case of crime, damages, hindrance, or disturbance of public order. In this case, mandatory supervision of the police department is not required.[177]

4.2.1.3 Enclosed areas not accessible to the public

The placement of surveillance cameras by a natural person for personal or domestic use inside a private residence does not have to be notified to the police department. This exemption also applies to the keeping of a register of processing activities and the placement of a pictogram.[178]

4.2.2 Mobile surveillance cameras

The general obligations for fixed and temporarily fixed surveillance cameras also apply to mobile cameras. Consequently, this section will only discuss the relevant differences.

4.2.2.1 Non-enclosed areas

Mobile surveillance cameras may only be used by municipal governments in non-enclosed areas in the context of automatic license plate recognition, and for the purpose of (1) prevention, detection or tacking of hindrance or (2) verifying the adherence to municipal regulations relating to payed parking. The use of mobile surveillance cameras for these purposes requires a positive assessment of the municipal council.[179]

The presence of mobile surveillance cameras must be announced through the placement of a pictogram on the vehicle to which the mobile camera is attached, in combination with any other information channel to clearly inform civilians.[180]

4.2.2.2 Enclosed areas

For enclosed areas, mobile surveillance cameras may only be used by a controller in three specific situations: (1) in the context of the legislation on private and special security, (2) in an enclosed area where nobody is presumed to be present, and (3) by a natural person for personal or domestic use, in an enclosed area not accessible to the public.[181] In the first two situations, the controller must place a pictogram at the entrance of the surveilled area, in order to notify individuals of the presence of camera surveillance.[182]

4.2.3 Common provisions

Some provisions of the Camera Act apply to surveillance cameras in general, regardless of the specific type.

First of all, all covert uses of surveillance cameras is prohibited. The Act describes ‘covert use’ as any use of surveillance cameras without prior consent of the person being filmed, or for mobile cameras in

[176] Ibid.
[177] Article 6, (3) of the Act of 21 March 2007 regulating the installation and use of surveillance cameras.
[178] Article 7, (2) of the Act of 21 March 2007 regulating the installation and use of surveillance cameras.
[179] Article 7/1 of the Act of 21 March 2007 regulating the installation and use of surveillance cameras.
[180] Article 7/3, (2) of the Act of 21 March 2007 regulating the installation and use of surveillance cameras.
[181] Article 7/2 of the Act of 21 March 2007 regulating the installation and use of surveillance cameras.
[182] Article 7/3, (2) of the Act of 21 March 2007 regulating the installation and use of surveillance cameras.

non-enclosed areas, if they do not respect the information obligation by making use of a pictogram. Entering an area that makes the use of video surveillance known through a pictogram is considered as valid prior consent.[183]

The Belgian Camera Act also deals with the use of smart surveillance cameras. Article 8/1 clarifies that the use of smart surveillance cameras which are linked to registers or files of personal data is only allowed for the purpose of automatic license plate recognition. They are defined as surveillance cameras that have parts or software which enable it to autonomously process collected images.[184]

For publicly accessible enclosed areas and enclosed areas not accessible to the public, only the controller or the person acting under authority of the controller has access to the footage. The controller must take all necessary security measures to protect the footage against unauthorized access. Persons that have authorized access to the footage have a discretion obligation regarding the personal data derived from the footage. There are, however, specifically defined situations in which the controller can, or must, transfer the footage to law enforcement authorities.[185] In addition, every person that has been filmed has a right of access to the video footage. The data subject must send an access request to the controller in conformity with data protection legislation, while providing sufficiently detailed information to localize the footage in question.[186]

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.[187] Capturing images aimed at providing biometric information is not prohibited, because sometimes facial images may qualify as biometric data.

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

5 Web analytics scenario

This use-case addresses the privacy-preserving computation of data-analytics, with a focus on statistics over large amounts of usage data. Analytics on access pattern data of web services can be used for various purposes, such as providing better suggestions and optimizing the performance of the service.[188]

Awless is an open-source command line interface used by AWS developers (f.e. code and system developers) that allows the creation, update and deletion of resources on Amazon Web Services. The use of functional encryption enables developers to gather data such as website access counts and perform statistical analysis upon them such that the data themselves are never available in unencrypted form to any party other than the originators of the data.[189]

This section aims to identify relevant legal requirements derived from the applicable legislation, namely; the GDPR, the eCommerce Directive, and the ePrivacy framework. These requirements will primarily apply to the end-use of the data analytics tool, since the data used in the research phase and development of the prototypes is synthetic.

5.1 The General Data Protection Regulation (GDPR)

Analytics of web service usage data will often involve the processing of personal data, such as; IP-addresses[190], the location of terminal equipment, and other identifying user information. These processing activities will trigger the scope of the GDPR, thereby imposing obligations provider of the web service.

This section identifies the legal requirements of the GDPR that are particularly relevant for the web analytics use-case, which apply in addition to the general GDPR requirements (f.e. data subject rights, data protection by design, DPIA, etc.).

5.1.1 Data protection principles (art. 5 GDPR)

5.1.1.1 Lawfulness, fairness and transparency (art. 5, (a) GDPR)

The principle of lawfulness, which imposes the requirement to rely on a legitimate legal ground for processing activities, will be discussed below (Section 5.1.2).

Firstly, fairness of processing relates to the relationship between the controller and data subject. It is a broad concept that goes beyond mere transparency obligations. The processing of personal data should be done in an ethical manner; the controller must properly inform the data subject, in a transparent manner, of the processing activities and accompanying risks. Compliance with the GDPR should be demonstrated to the data subject and the data subject should have a good understanding of what is happening with their personal data.[191]

Secondly, the processing must be done in a transparent manner in relation to the data subject. This means that the controller must provide the necessary information in a transparent way, including; the

[188] D3.1 Technical Requirement Analysis Report, FENTEC Consortium, May 2018, 18-19.
[189] Ibid., 19-21.
[190] Court of Justice of the European Union, *Patrick Breyer v Bundesrepublik Deutschland*, Judgement of 19 October 2016, C-582/14, para. 49.
[191] The European Union Agency for Fundamental Rights, the Council of Europe, and the European Data Protection Supervisor, " Handbook on European data protection law", 2018, 118-119.

information provided to the data subject before the processing starts[192], information that should be available during the processing, and information related to a request of access[193].[194] This information should be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language.[195] The data subject should be aware of the risks, rules, safeguards, and rights relating to the processing of their personal data. The provider of the web service making use of Awless must therefore inform the data subject in accordance with articles 12, 13, and 14 GDPR.

5.1.1.2 Purpose limitation (art. 5, (b) GDPR)

Personal data may only be collected for specified, explicit and legitimate purposes. Further processing of personal data is only allowed in a manner that is compatible with the initial purposes, which can be assessed on the basis of a compatibility test under article 6, 4 of the GDPR. The end-use of the web analytics tool would, for example, collect and process personal data in order to optimize the performance of the service. In such a case, the processing activities must be limited to that specific purpose or another compatible purpose. Under article 5, (b) of the GDPR, statistical purposes are considered to be compatible with the initial purposes.[196] It is, however, still advisable to conduct a compatibility assessment in order to avoid any risk of unlawful processing. This is important for the web analytics use-case because a statistical analysis will be performed on the data.

5.1.1.3 Data minimisation and storage limitation (art. 5, (c) and (e) GDPR)

The principle of data minimisation determines that the personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. The specific application of this principle will depend on the purposes of processing. Since the web-analytics technology will be used to improve the performance of the service, all processed personal data should be relevant and contribute to this purpose.

The storage limitation principle prescribes that personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes of processing. This means that, in case of web-analytics, personal data may only be stored for as long as is necessary to achieve the purpose of improving the performance of the service. Personal data that is processed solely for statistical purposes may be stored for longer periods on the condition that appropriate technical and organisational measures are implemented, such as functional encryption and clear storage policies.

5.1.1.4 Integrity and confidentiality (art. 5, (f) GDPR)

Personal data must be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. Appropriate technical or organisational measures must be implemented in order to ensure the integrity and confidentiality of personal data. Functional encryption contributes to this objective of security, specifically the confidentiality of personal data.

[192] Articles 13 and 14 of the GDPR.
[193] Article 15 of the GDPR.
[194] The European Union Agency for Fundamental Rights, the Council of Europe, and the European Data Protection Supervisor, " Handbook on European data protection law", 2018, 120.
[195] Article 12 of the GDPR.
[196] The European Union Agency for Fundamental Rights, the Council of Europe, and the European Data Protection Supervisor, " Handbook on European data protection law", 2018, 125.

5.1.2 Lawfulness of processing (art. 6 GDPR)

The requirement of 'lawfulness' is a data protection principle which makes clear that the processing of personal data must be based on, and limited to, a legitimate legal ground. Two legal grounds are of particular relevance to the use of the web analytics tool.

5.1.2.1 Consent (art. 6, (a) GDPR)

Consent is the first viable legal basis for the processing of personal data through the web analytics tool.

In order to obtain valid consent from the data subject, it must be freely given, specific, informed and unambiguous. Furthermore, the request for the data subject's consent must be clearly distinguishable as such and it must be presented in an intelligible and easily accessible form, using clear and plain language. The controller must be able to demonstrate that the data subject has consented, and it must also be made clear to the data subject that consent can be withdrawn at any time.[197] Consent may not always be the most desirable legal basis due to its strict requirements and the ability of the data subject to withdraw consent. In the case of web analytics, consent will most likely be obtained through the terms and conditions of the web service provided by the AWS developer.

In the case of web analytic services, which can be qualified as 'information society services', additional conditions apply when consent is obtained from a child. Such consent shall only be lawful where the child is at least 13 to 16 years old, depending on Member State law. Where the child is below this age, consent must be given or authorized by the holder of parental responsibility over the child.[198] [199]

5.1.2.2 The legitimate interests pursued by the data controller or third party (art. 6, (f) GDPR)

The legitimate interest of the controller or third party may also serve as a viable legal basis for the use of the web analytics tool.

The existence of a legitimate interest must be assessed on a case-by-case basis. Firstly, an identified interest must be real, present and sufficiently specific; it must be something that relates to current or near-future activities. When an interest is too vague or speculative, it will not be sufficient to act as a legal ground. Secondly, the nature of the legitimate interest may vary; it can include individual interests, commercial interests, or a societal interest. Thirdly, the interest must be lawful, i.e. respect EU and national law.[200]

Due to the flexibility of this legal basis, it is difficult to make a general prior assessment for a specific interest. Some purposes have been acknowledged as possible legitimate interests under article 6, (f) of the GDPR (f.e. physical, IT, and network security, direct marketing, preventing fraud and misuse of services, etc.).[201] The use of web analytics in order to improve the performance of a service may qualify as a legitimate interest if the abovementioned conditions are met. This legal basis may therefore be applicable to the end-use of the web analytics service.

This legal basis also requires the processing to be necessary for the purposes of the legitimate interest and there must be a balancing exercise between the interests of the controller and the interests or

[197] Article 4 (11), 7 and recital (32) of the GDPR.
[198] Article 8 of the GDPR.
[199] Article 29 Working Party, Guidelines on consent under Regulation 2016/679, adopted on 28 November 2017, last revised and adopted on 10 April 2018, 23-24.
[200] Article 29 Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, adopted on 9 April 2014, 24-25.
[201] Ibid., 25.

fundamental rights and freedoms of the data subject. These concepts are explained in more detail under Section 4.1.1.1.

5.2 The Electronic Commerce Directive (eCommerce Directive)

The applicability of the eCommerce Directive[202] has been briefly described in D3.2, Section 5.2.

The eCommerce Directive applies to information society services (ISSs), which can be defined as "services normally provided for remuneration, (1) at a distance, (2) by electronic means, and (3) at the individuals request of a recipient of services."[203] The service developed in the web analytics use-case satisfies all of these elements. It is a service provided at a distance, meaning that the parties are not simultaneously present. The service is provided by electronic means, since it is sent and received by means of electronic equipment and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means. Lastly, the service is provided at the individual request of a recipient of services, meaning through the transmission of data on individual request. In the web analytics use-case, the recipient is the AWS developer making use of the web analytics service for the management of its web service.

The applicability of the eCommerce Directive gives rise to certain obligation on the part of the ISS provider. The obligations arising from the Directive are further implemented in Member State law.

5.2.1 Information requirement

The provider of an ISS must render easily, directly and permanently accessible specific information to the recipients of the ISS. In the web analytics use-case the provider of the web analytics tool will be bound by the obligation to inform the recipient of the service (i.e. the AWS developer). The information to be provided includes:

a) the name of the service provider;
b) the geographic address at which the service provider is established;
c) the details of the service provider, including his electronic mail address, which allow him to be contacted rapidly and communicated with in a direct and effective manner;
d) where the service provider is registered in a trade or similar public register, the trade register in which the service provider is entered and his registration number, or equivalent means of identification in that register;
e) where the activity is subject to an authorisation scheme, the particulars of the relevant supervisory authority.[204]

[202] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce).
[203] Article 1, (b) of Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (codification).
[204] Article 5 of the eCommerce Directive.

In case the ISS refers to prices, they have to be indicated clearly and unambiguously and whether they are inclusive of tax and delivery costs.[205] This obligation does not apply to the present use-case due to the open-source nature of the web analytics tool.

5.2.2 Commercial communications

In the context of commercial communications, the provider of the web analytics tool must ensure that:

a) the commercial communication shall be clearly identifiable as such;
b) the natural or legal person on whose behalf the commercial communication is made shall be clearly identifiable.[206]

Unsolicited commercial communications by electronic mail must also be identifiable clearly and unambiguously as such, as soon as it is received by the recipient.[207] These obligations are not as relevant in the present use-case due to the open-source nature of the web analytics tool.

5.2.3 Electronic contracts

The provision of a service on the basis of an electronic contract gives rise to additional obligations for the provider of an ISS. However, these obligations do not apply when agreed by parties who are not consumers. A consumer is any natural person who is acting for purposes outside his or her trade, business or profession.[208]

First of all, the service provider must provide the necessary information in a clear, comprehensive, and unambiguous way, prior to the order being placed. This information includes: (a) the different technical steps to follow to conclude the contract, (b) whether or not the concluded contract will be filed by the service provider and whether it will be accessible, (c) the technical means for identifying and correcting input errors prior to the placing of the order, and (d) the languages offered for the conclusion of the contract.[209]

Secondly, when an order is placed through technological means, the service provider has to acknowledge the receipt of the order without undue delay and by electronic means. They are deemed to be received when the parties to whom they are addressed are able to access them. Effective and accessible technical means must be available to identify and correct input errors prior to the placing of the order.[210]

[205] Article 5, 2 of the eCommerce Directive.
[206] Article 6 of the eCommerce Directive.
[207] Article 7 of the eCommerce Directive.
[208] Article 2, (e) of the eCommerce Directive.
[209] Article 10 of the eCommerce Directive.
[210] Article 11 of the eCommerce Directive.

5.3 The ePrivacy framework

5.3.1 The ePrivacy Directive

The general obligations derived from the ePrivacy Directive[211] apply to the processing of personal data with regards to the provision of publicly available electronic communications services in public communications networks in the EU.[212]

An electronic communications service is defined as "*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.*"[213]

The web analytics service as described in the current use-case does not fall within the scope of this definition, since it does not consist *"wholly or mainly in the conveyance of signals"*. The primary function of the web analytics service is to perform analytics on usage data, rather than the conveyance of signals. Consequently, most obligations that apply to providers of electronic communications services will not be applicable to the present web analytics use-case.

One obligation that remains relevant for the web analytics use-case relates to the terminal equipment of users. According to article 5, 3 of the ePrivacy Directive, the application of which is not limited to electronic communications services, clarifies that the storing of information, or the access to information already stored, in the terminal equipment of a user is only allowed on if consent has been obtained from the user. The concept of consent under the ePrivacy Directive is the same as under the GDPR, meaning that consent must be freely given, specific, informed, and unambiguous.[214] The user must also receive clear and comprehensive information in accordance with the GDPR, including about the purposes of processing. Consent does not have to be obtained in case (1) the technical storage or access is for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or (2) it is strictly necessary in order for the provider of an ISS, which is explicitly requested by the user, to provide the service.[215] For the web analytics use-case, this means that consent has to be obtained from the user of the web service in order to place cookies on their terminal equipment, unless one of the two exceptions apply. This is an obligation for the provider of the web service which makes use of the web analytics tool, insofar this tool places cookies.

5.3.2 The ePrivacy Regulation

On the 10th of January 2017, the European Commission released its proposal for a new ePrivacy Regulation [216] replacing the 2002 ePrivacy Directive in the electronic communication sector. More than

[211] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).
[212] Article 3 of the ePrivacy Directive.
[213] Article 2 of Directive 2002/58/EC; article 2, (c) of Directive 2002/21/EC.
[214] Recital 17 of the ePrivacy Directive; article 94 of the GDPR; recital 32 of the GDPR.
[215] Article 5, 3 of the ePrivacy Directive.
[216] See, for the original text proposed by the European Commission: Proposal for a Regulation of the European Parliament and the Council concerning the respect for private life and the protection of personal data in electronic

a mere updating exercise, the Commission's draft suggested to drastically broaden the scope of a normative framework which, until today, mainly focused on telecommunications. Being an integral part of the Digital Single Market strategy, the main objective of the proposal is to provide a high level of privacy protection for users of electronic communications services and a level playing field for all market players. As such, the text deals with various issues, ranging from the confidentiality, storage and erasure of communications to incoming call blocking and marketing communications. While it was initially expected to be finalized before May 2018 – matching the GDPR's entry into force – the text is still under ongoing negotiations within the Council.

On 22 November 2019, the Council has rejected the latest version of the ePrivacy Regulation[217]. More than two years after the initial proposal, there is still no consensus between Member States on several issues. In December 2019, the European Commission announced that it will present a revised ePrivacy proposal as part of the Croatian Presidency of the EU. As a result of these developments, it is still unclear when, or whether, the ePrivacy Regulation will be accepted. Considering the continuous changes in scope and subject matter, a further analysis will be done when more certainty exists.

communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) [10 January 2017] 2017/0003(COD) <https://data.consilium.europa.eu/doc/document/ST-5358-2017-INIT/en/pdf> accessed 10 December 2019.

[217] The version of 8 November 2019 <https://data.consilium.europa.eu/doc/document/ST-13808-2019-INIT/en/pdf> accessed 10 December 2019.

6 Conclusion

In this deliverable, applicable legal requirements were identified and summarized in a requirements monitoring table.

The second chapter laid down the overarching privacy, data protection, and cybersecurity features applicable to the FENTEC project and its use-cases. It gave an overview of the generally applicable requirements derived from the GDPR, such as; the data quality principles, privacy and data protection by design, security requirements, and the relevance of a DPIA. Secondly, the new Cybersecurity Act was analysed. This framework does not, currently, contain requirements for FENTEC, but will soon give rise to certification schemes that could apply to FENTEC technologies.

The third, fourth, and fifth chapters set out the legal requirements for the three use-cases; the digital currency scenario, the video surveillance scenario, and the web analytics scenario.

For the digital currency scenario, legal requirements were derived from the Second E-money Directive, the Second Payment Services Directive, the Fourth and Fifth Anti-money Laundering Directives, and the GDPR. Due to the fragmented nature of the sector-specific legal framework, many different applicable laws and requirements were identified.

The identification of requirements for the video surveillance scenario is, due to a lack of sector-specific legislation, limited to the GDPR and national law. In this context, the Belgian Camera Act was used as an example to identify possible national requirements.

The requirements for the web analytics scenario are, similar to the video surveillance scenario, more limited. This chapter presented specific GDPR requirements, which apply in addition to the general requirements, as well as the requirements derived from the eCommerce Directive. It also contained a short section on the ePrivacy framework, insofar it applies to this specific scenario. Due to the constant changes and developments in the ePrivacy negotiations, the applicability and relevant requirements of the ePrivacy Regulation will be further analysed in D3.4, together with future certifications schemes under the Cybersecurity Act, the Machinery Directive (2006/42/EC), the Open Data Directive (2019/1024), and the liability and accountability frameworks.

Finally, the requirements monitoring table in the Annex provides an overview of all applicable legal requirements, accompanied with relevant implementation guidelines, their priority, and categorisation.

The next steps will be to monitor and validate the implementation of the identified legal requirements, as well as acknowledge legal and policy developments that should be taken into account. This work will result in D3.4, which will include any newly identified requirements.

Annexes

Table of requirements and implementation guidelines

Table 1: Overarching features

	Legal requirement specification		Implementation guidelines	Priority		Category		
				research	**post-research**	**mandatory**	**desirable**	**optional**
R1	Personal data	GDPR art. 4(1)	Any information relating to an identified or identifiable natural person ('data subject').		x	x		
R2	Data protection by design and by default	GDPR art. 25	Technical and organisational measures to ensure data protection and privacy by design and by default.	x	x	x		
R3	Security measures and security by design	GDPR art. 32, 34	Technical and organisational measures to ensure data security by design, including procedure for notification of data breaches.	x	x	x		
R4	Data quality principles	GDPR art. 5	Support and implementation of data quality principles: lawfulness, transparency and fairness; purpose limitation, data minimisation, data accuracy, integrity and confidentiality, storage limitation.	x	x	x		
R5	Lawfulness	GDPR art. 6	Ensure that valid legal grounds are given for data processing.		x	x		
R6	Accountability and general responsibility of the controller	GDPR art. 5(2) and 24	Implement technical and organisational measures to ensure and demonstrate compliance, such as appointing a DPIA, logging internal data procedures, etc.					

R7	Data protection impact assessment	GDPR art. 35	Minimum content: - Description of processes, procedures, purposes and goals - Necessity and proportionality - High risks to rights and freedoms of individuals - Counter-measures and safeguards If relevant, consult DPO.	x	x		x	

Table 2: Digital currency scenario

	Legal requirement specification		**Implementation guidelines**	**Priority**		**Category**		
				research	**post-research**	**mandatory**	**desirable**	**optional**
R1	Electronic money issuing	EMD2 art. 1(1)	Ensure that adopters comply with definition of electronic money issuers.		x	x		
R2	Payment services (PS)	PSD2 Annex I	Ensure that the use of digital coin/digital currency complies with definition of payment services.		x	x		
R3	Payment services provider (PSP)	PSD2 art. 4(11)	Ensure that adopters comply with definition of payment services providers.		x	x		
R4	Sensitive payment data	PSD2 art. 4(32)	Data, including personalised security credentials which can be used to carry out fraud. Ensure safe storage and appropriate division of keys.			x		
R5	Authorisation of payments: consent and withdrawal of consent	PSD2 art. 64	Ensure user consent is collected and documented. Ensure consent can be withdrawn within the prescribed time limit	x	x	x		

			(irrevocability criterion).					
R6	Data access by PISPs and AISPs	PSD2 art. 66-67	Ensure that relevant third parties may access relevant data without enabling screen scraping.	x	x	x		
R7	PS user's obligations regarding personalised security credentials	PSD2 art. 69	Notify the user about the obligations they have regarding personalised security credentials.		x	x		
R8	Obligations of the PSP in relation to payment instruments	PSD2 art. 70	Ensure that the personalised security credentials are only accessible to the entitled user. Do not send unsolicited payment instruments. Ensure retrieval and cancellation procedures.	x	x	x		
R9	Notification and rectification of unauthorised or incorrectly executed payment transactions	PSD2 art. 71	Ensure user can ask for rectification.			x		
R10	Evidence on authentication and execution of payment transactions	PSD2 art. 72	Keep records.	x	x	x		
R11	PSP's liability for unauthorised payment transactions	PSD2 art. 73	Enable refund unless fraud is suspected.		x	x		
R12	Management of operational and security risks	PSD2 art. 95	Implement mitigation measures and control mechanisms to manage the operational and security risks. Report mechanisms regularly to the competent authority.		x	x		
R13	Incident reporting	PSD2 art. 96	Notify competent authority in case of		x	x		

			major operational and security incident. Notify PS users of any impact on their financial interests.					
R14	Authentication	PSD2 art. 97	Apply strong customer authentication. Two factor authentication for payments above EUR 30.	x	x	x		
R15	Transparency and information obligations	PSD2 art. 44-49	Provide relevant pre- and post-contractual information.		x	x		
R16	Data protection in PS	PSD2 art. 94, GDPR art. 5, 6, 7, 9	Obtain (explicit) consent, where appropriate, especially in profiling/automated decision-making and/or sensitive personal data. Otherwise: ensure other valid legal grounds, for example for third party silent data processing, screen scraping, etc. Ensure purpose limitation, data minimisation and information obligations.	x	x	x		
R17	Liability	PSD art. 20	Liability for third parties, employees, outsourced services, etc.		x	x		
R18	Money laundering (ML)	MLD IV art. 1(3), MLD V art. 1(3)	Intentional committing of certain crimes.		x	x		
R19	Property	MLD IV art. 3(3), MLD V art. 3(3)	Assets of any kind, whether corporeal or incorporeal, movable or immovable, tangible or intangible, and legal documents or instruments.		x	x		
R20	Politically exposed persons (PEPs)	MLD IV art. 3(9), MLD V art. 3(9)	A natural person who is or who has been entrusted with prominent public functions.		x	x		

R21	Customer due diligence (CDD) – know your client (KYC)		Regular CDD - Prohibition of anonymous accounts - Timing - Exemptions - Mitigating measures - Verification of identity and minimum content Simplified CDD - National legislation - Lower risk factors in Annex II (customer, transaction, geographic…) Enhanced CDD - Higher risk factors (PEPs, third countries …) - Perform risk assessment to ensure digital coin is not used in higher risk situations.		x	x		
R22	Reporting	MLD IV art. 33, 37, 39, MLD V art. 33, 37, 39	Provide relevant information to FIUs. Do not disclose the reporting to the client.		x	x		
R23	Data protection in AML	MLD IV art. 40-44, MLD V art. 40-44	Purpose limitation principle: collection, analysis, storage and sharing of data only for the purposes of preventing money laundering and terrorist financing; customer due diligence, ongoing monitoring, investigation and reporting. Strict necessity. Link to GDPR – *lex specialis.*	x	x	x		

			Limit keeping of documents to 5 (+5 if national law) years. No processing for commercial purposes.					
R24	Proportionality	MLD IV art. 41(2), MLD V art. 41(2), Digital Rights Ireland - Joined Cases C-293/12 and C-594/12	Risk assessment approach. Strict necessity in ensuring purpose limitation.		x	x		
R25	Personal data and sensitive payment data	GDPR art. 4(1), PSD2 art. 4(32)	Appropriate division of keys between actors.		x	x		
R26	Data quality principles	GDPR art. 5	Disclosure of relevant information. Ensure relevant legal grounds exist. Appropriate division of keys to ensure data minimisation. Use functional encryption.	x	x	x		
R27	Legal grounds for data processing	GDPR art. 6	User consent. Necessary to perform a contract. Necessary for a task performed in the public interest.		x	x		
R28	Relationship with processor	GDPR art. 28	Due diligence in choice. Adopt a contract.		x	x		
R29	Right to access	GDPR art. 15	Restricted access. Appropriate division of keys to ensure exercise of this right.		x	x		
R30	Right to data portability	GDPR art. 20	Ensure data may be transferred to another provider.		x	x		
R31	Data protection and data security by design	GDPR art. 5, 24, 25, 32	Organisational and technical measures. Functional encryption, no default passwords,	x	x	x		

			company-wide cyber-security culture, etc. Link to NIS Directive – incident reporting.					
R32	Data protection impact assessment	GDPR art. 35, 36	Required for KYC/CDD or if other high risks are present.		x	x		
R33	Data protection officer	GDPR art. 37, 38	Suggested for KYC/CDD adopters.		x		x	

Table 3: Video surveillance scenario

	Legal requirement specification		**Implementation guidelines**	**Priority**		**Category**		
				research	**post-research**	**mandatory**	**desirable**	**optional**
R1	Legal grounds for processing personal data	GDPR art. 6	Legitimate interest of the controller. Task carried out in the public interest or in exercise of official authority. Legal obligation.		x	x		
R2	Legal grounds for processing of special categories of personal data	GDPR art. 9	Substantial public interest. Vital interests of data subject.		x	x		
R3	Data minimisation	GDPR art. 5	Processing of surveillance footage must be adequate, relevant, and limited to what is necessary for processing purpose.		x	x		
R4	Storage limitation	GDPR art. 5	Surveillance footage data must be kept in a form which permits identification for no longer than is necessary for processing purpose.		x	x		

R5	Transparency	GDPR art. 12	Provide necessary information in a transparent way; two layers of information (f.e. warning sign and second channel).		x	x		
R6	Information obligation	GDPR art. 13	Provide necessary information to the data subject.		x	x		
R7	Right of access	GDPR art. 15	Provide access to surveillance. footage and necessary information. Provide copy of surveillance footage.		x	x		
R8	Right of erasure	GDPR art. 17	Erase surveillance footage of data subject on basis of legitimate ground.		x	x		
R9	Right of restriction	GDPR art. 18	Restrict processing of personal data in specified cases.		x	x		
R10	Right to data portability	GDPR art. 20	Ensure that surveillance footage may be transferred to another controller.		x	x		
R11	Right to object	GDPR art. 21	Cease processing of surveillance footage on basis of one of the legitimate grounds.		x	x		
R12	Appropriate technical and organizational measures	GDPR art. 5, 24, 25, 32	Implement appropriate technical and organizational measures (e.g. DPIA, access policies, encryption, scrambling and editing software, limitation on analytics, etc.).		x	x		

R13	Data protection impact assessment	GDPR art. 35	Conduct a DPIA in case of (1) systematically monitoring a publicly accessible area or (2) processing of special categories of data on a large scale.		x	x		
R14	Notification obligation	Belgian Camera Act art. 5 (3), 6 (2), 7 (2), 7/3 (1)	The decision to place a surveillance camera must be notified to the police department.		x	X		
R15	Record keeping	Belgian Camera Act art. 5 (3), 6 (2), 7 (2), 7/3 (1)	The controller must keep a register with processing activities of surveillance cameras.		x	X		
R16	Municipal approval	Belgian Camera Act art. 5 (2), 7/1, 8/2	In the specified cases, the placement of a surveillance camera requires a positive assessment of the municipal council.		x	X		
R17	Placement of a pictogram	Belgian Camera Act art. 5 (3), 6 (2), 7 (2), 7/4 (2)	The controller must place a pictogram to signal the presence of camera surveillance.		x	X		
R18	Targeted area of surveillance	Belgian Camera Act art. 5 (3), 6 (2), 7 (2), 8/2	The controller must ensure that the surveillance camera is not aimed at an area for which the controller does not process data, unless specific circumstances apply (e.g. consent and restricted surveillance).		x	X		

R19	Viewing of real-time surveillance footage	Belgian Camera Act art. 5 (4), 6 (3), 7 (3), 7/3 (3)	Viewing footage in real-time is only allowed in order to intervene in case of crime, damages, hindrance or disturbance of public order. Modalities will apply depending on the type of surveillance camera and surveilled area.		x	X		
R20	Recording surveillance footage	Belgian Camera Act art. 5 (4), 6 (3), 7 (3), 7/3 (4)	Recording surveillance footage is only allowed in order to collect evidence of hindrance, crime or damages, and to track and identify offenders, disturbers of the public order, witnesses, or victims. The footage must be deleted after one month if it does not contribute to these purposes.		x	X		
R21	Placement of a public display	Belgian Camera Act art. 6 (2)	The controller may place a display that publicly shows the real-time video footage of the fixed/temporarily fixed surveillance cameras in a publicly accessible enclosed area.		x			x
R22	Use of mobile surveillance cameras in non-enclosed areas	Belgian Camera Act art. 7/1	Mobile surveillance cameras may only be used by municipal governments in non-enclosed areas for the specified purposes.		x	X		
R23	Use of mobile surveillance cameras in enclosed areas	Belgian Camera Act art. 7/2	Mobile surveillance may only be used in enclosed spaces in specified cases.		x	X		

R24	Prohibiton of covert use	Belgian Camera Act art. 8	All covert uses of surveillance cameras is prohibited.		x	X		
R25	Use of smart surveillance cameras	Belgian Camera Act art. 8/1	Smart surveillance cameras linked to registers/files of personal data may only be used for automatic license plate recognition.		x	X		
R26	Access to surveillance footage	Belgian Camera Act art. 9, 12	For publicly accessible enclosed areas and enclosed areas not accessible to the public, only the controller and person acting under authority of the controller has access to the footage. The data subject also has a right of access.		x	X		
R27	Security measures	Belgian Camera Act art. 9	The controller must take all necessary security measures to protect the footage against unauthorized access.		x	X		
R28	Discretion obligation	Belgian Camera Act art. 9	Persons that have authorized access to the footage have a discretion obligation regarding the personal data derived from the footage.		x	X		
R29	Special categories of personal data	Belgian Camera Act art. 10	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.		x	x		

Table 4: Web analytics scenario

	Legal requirement specification		Implementation guidelines	Priority		Category		
				research	post-research	mandatory	desirable	optional
R1	Data protection principles	GDPR art. 5	Provide relevant information in a transparent way. Limit collection and processing of personal data to what is necessary for specific purpose. Implement appropriate technical and organizational measures to ensure security of personal data (f.e. functional encryption).		x	x		
R2	Legal grounds for processing personal data	GDPR art. 6	Obtain valid consent from data subject. Legitimate interest of the controller or third party.		x	x		
R3	General information obligation	eCommerce Directive art. 6	The provider of an ISS must provide the necessary information to the recipient of an ISS.		x	x		
R4	Commercial communications	eCommerce Directive art. 6 and 7	Ensure that the commercial communication and unsolicited commercial communication satisfy the applicable conditions.		x	x		

R5	Electronic contracts	eCommerce Directive art. 10 and 11	In the context of an electronic contract, the provider of an ISS must provide the necessary information to the recipient of an ISS. The provider of an ISS must also apply the applicable principles in case the recipient places an order through technological means.		x	x		
R6	Cookies	ePrivacy Directive art. 5	The provider of the web service making use of the web analytics tool must obtain consent from the user, unless one of the exceptions apply.		x	x		