KRAKEN

BROKERAGE AND MARKET PLATFORM FOR PERSONAL DATA

D2.1 Ethical and Legal Framework Report

www.krakenH2020.eu

This project has received funding from the European Union’s Horizon 2020 (H2020) research and innovation programme under the Grant Agreement no 871473

D2.1 Ethical and Legal Framework Report

Grant agreement	871473
Work Package Leader	INFOCERT
Author(s)	Wim Vandevelde (KU Leuven)
Contributors	Jessica Schroers (KU Leuven), Danaja Fabčič Povše (KU Leuven), Stefan Schauer (AIT), and Martin Latzenhofer (AIT)
Reviewer(s)	Alfonso Carcasona Prats (INFOCERT) and Rob Holmes (TEX)
Version	Final
Due Date	31/08/2020
Submission Date	31/08/2020
Dissemination Level	Public

Release History

Version	Date	Description	Released by
V0.1	13/03/2020	Table of Contents	Wim Vandevelde (KU Leuven)
V0.2	30/06/2020	First draft version	Wim Vandevelde (KU Leuven)
V0.3	21/07/2020	Table of Contents for section 4 ‘Privacy Metrics’	Martin Latzenhofer (AIT) and Stefan Schauer (AIT)
V0.4	31/07/2020	Final draft version	Wim Vandevelde (KU Leuven)
V0.5	19/08/2020	Review and finalization of section 4 ‘Privacy Metrics’	Stefan Schauer (AIT)
V0.6	21/08/2020	Review feedback by partners INFOCERT and TEX	Alfonso Carcasona Prats (INFOCERT) and Rob Holmes (TEX)
V0.7	26/08/2020	Final version	Wim Vandevelde (KU Leuven)
V1.0	31/08/2020	Submitted version	Atos

Table of Contents

List of Figures

List of Acronyms

Acronym	Description
CFREU	Charter of Fundamental Rights of the European Union
CJEU	Court of Justice of the European Union
D2.1	Deliverable 2.1
D7.2	Deliverable 7.2
DPO	Data Protection Officer
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
eIDAS	Electronic Identification and Trust Services
eIDs	Electronic Identification Scheme
GDPR	General Data Protection Regulation
KRAKEN	broKeRage And marKEt platform for persoNal data
KYC	Know Your Customer
LoA	Level of Assurance
PETs	Privacy Enhancing Technologies
SSI	Self-Sovereign Identity
T2.1	Task 2.1
T7.2	Task 7.2
TSP	Trust Service Provider
WP2	Work Package 2
WP7	Work Package 7

Executive Summary

The development and use of KRAKEN (broKeRage And marKEt platform for persoNal data) technology falls under the scope of several legal regimes, such as the data protection and electronic identification frameworks. These legal frameworks give rise to numerous legal requirements and obligations which have to be taken into account in the development and design of new technologies. This deliverable falls under Task 2.1 (T2.1) 'Applicable legal framework and ethical principles and privacy metrics', which is the first task of Work Package 2 (WP2) 'Technical aspects and architecture specifications'. It aims to identify and analyze the applicable legal frameworks in order to provide a high-level overview of principles which need to be taken into account in the course of the project and the development of technologies. The results of this deliverable will be used for the subsequent elicitation of ethical and legal requirements, which will be performed in Task 7.2 (T7.2) 'Ethical and Legal Analysis and Evaluation' under Work Package 7 (WP7) 'Ethical and Legal compliance'. The resulting deliverable of this task, Deliverable 7.2 (D7.2) 'Ethical and legal requirement specification', will provide a more in-depth analysis of the legal requirements and accompanying implementing guidelines for KRAKEN.

The applicable privacy and data protection framework can be divided in primary and secondary sources. Firstly, the primary sources exist on the most fundamental level. The fundamental rights to privacy and data protection can be found in both the European Convention on Human Rights and the Charter of Fundamental Rights of the European Union. These two legal instruments have influenced each other throughout the years and the protection of these rights are similar in both documents. Although both fundamental rights to privacy and data protection overlap in some way, they should not be seen as identical rights. Their scope of application differs and an infringement of one of these rights does not automatically lead to an infringement of the other. The importance of these fundamental rights cannot be understated, as illustrated by their influence on secondary legislation.

Secondly, the General Data Protection Regulation (the GDPR), which is a secondary source of EU law, has greatly changed the data processing landscape in the EU. Its scope of application is quite broad and can be confusing at times, defining several different concepts, such as; 'processing', 'personal data', 'identifiability', 'data subject', 'controller', and 'processor'. In the end, it is clear that the scope depends on seemingly abstract assessments, which are in fact quite objective (e.g. what are 'means reasonably likely to be used'?). The GDPR lays down several core data protection principles which have to be respected at all times (i.e. lawfulness, fairness, and transparency, purpose limitation, data minimization, storage limitation, accuracy, integrity and confidentiality, and accountability). The spirit and importance of these principles can be seen throughout the entirety of the GDPR, such as the requirement for a legal basis for processing and the data subject rights. The most well-known legal basis, although not always the most desirable, is consent of the data subject. In KRAKEN, this legal basis will play an important role for the lawfulness of processing activities. It is also crucial to keep the protection of the data subject in mind. For this reason, the controller should take into account the potential risks of its processing activities. Depending on the extent of these risks, for example when processing sensitive personal data, the controller should implement appropriate technical and organizational measures to ensure the security of personal data. In the context of the protection of the data subject, it is also important for the data subject to be able to exercise his/her rights under the GDPR. In fact, the data subject enjoys several rights which can be addressed to the controller (e.g. the right of access, right to rectification, right to erasure, right to restriction of processing, right to data portability, and the right to object), even though some of these rights can also be restricted.

Thirdly, the Regulation on electronic identification and trust services for electronic transactions (the eIDAS Regulation) lays down rules on the mutual recognition and notification of electronic identification schemes between Member States and establishes a legal framework for trust services (e.g. electronic signatures, electronic seals, electronic time stamps, etc.). Particular attention must be

given to electronic signatures and their legal effects. The Regulation further specifies different types of electronic signatures (i.e. advanced electronic signature and qualified electronic signature) with each their own requirements and weight.

Finally, the concept of privacy metrics is also an essential element for the KRAKEN project. While technical in nature, privacy metrics contribute to the overall enjoyment of privacy by users and to the transparency of processing activities in a system. There are many different types of privacy metrics, each with their own objectives and requirements. As a result, it is important to identify relevant considerations and parameters for the selection of appropriate privacy metrics in KRAKEN.

1 Introduction

1.1 Purpose of the document

This deliverable falls under T2.1, which is the first task of WP2. It aims to identify and analyze the ethical and legal frameworks applicable to the KRAKEN project and developed technologies. It provides a high-level overview of ethical and legal principles which need to be taken into account in the course of the project and development of the KRAKEN platform. The main focus of this analysis will lie on data protection (e.g. the GDPR) and electronic identification (e.g. the eIDAS Regulation) frameworks. This deliverable will serve as a basis for the subsequent elicitation of ethical and legal requirements, which will be performed in T7.2, under WP7. The resulting deliverable of this task, D7.2, will provide a more in-depth analysis of the legal requirements and accompanying implementing guidelines for KRAKEN.

1.2 Structure of the document

In the first chapter, this report addresses the existing privacy and data protection framework in the broad sense. It starts by explaining the current state of the fundamental rights to privacy and data protection in Europe. This is followed by an overview and high-level analysis of the applicable secondary data protection legislation in the EU, namely the GDPR.

In the second chapter, an overview of the most important concepts and principles of the electronic identification framework is provided.

The third chapter of this deliverable provides high-level information on the concept of privacy metrics. It looks at the particular objectives and requirements of privacy metrics, followed by an overview of considerations and parameters for the selection of privacy metrics in KRAKEN.

2 Privacy and data protection framework

This chapter will give an overview of the main regulatory instruments applicable to the KRAKEN technology under the privacy and data protection regime in Europe. While the concepts of privacy and data protection are similar and often used as synonyms, different legal instruments may apply.

The overview starts by taking a look at the rights of privacy and data protection in their capacity as fundamental rights and then goes on to describe the applicable secondary legislation (i.e. the GDPR).

2.1 Fundamental rights to privacy and data protection

2.1.1 The right to privacy

2.1.1.1 The scope of the right to privacy

The right to privacy is a fundamental human right that has been incorporated in both the European Convention on Human Rights (ECHR)[1] and the Charter of Fundamental Rights of the European Union (CFREU)[2]. The phrasing and interpretation of the right to privacy is near-identical in both instruments:

> *"Everyone has the right to respect for his private and family life, his home and his correspondence."*[3]
>
> *"Everyone has the right to respect for his or her private and family life, home and communications."*[4]

On first sight, the scope of this provision might seem rather limited. However, the European Court of Human Rights (ECtHR) has given it a broad interpretation and has made clear that the definition is not in any way exhaustive.[5] The concept of 'private life' extends to the 'personal autonomy' of an individual, which includes one's physical integrity, bodily self-determination, sexual orientation, relations with other persons, and more. Additionally, an individual enjoys the right to privacy even in areas outside the conventional 'home'. This approach is consistent with the case law of the ECtHR, which states that there exists a *"zone of interaction of a person with others, even in a public context, which may fall within the scope of private life"*[6]

With regards to the personal scope of these rights, it is important to note that the rights contained in the ECHR are enjoyed by the citizens of the Contracting Parties (i.e. members of the Council of Europe). Any individual may seek protection of their rights by filing a complaint with the ECtHR, which is the interpreter and arbiter of the ECHR. In fact, the ECtHR has interpreted the Convention as imposing both negative and positive obligations upon the Contracting Parties.[7] The obligations contained in the CFREU, on the other hand, apply to the institutions of the European Union and to the 28 Member States when implementing EU law. An individual that has suffered damage resulting from action or inaction by an EU institution can directly go to the Court of Justice of the European Union (CJEU) General Court if it has affected the individual directly and individually.

[1] Council of Europe, Convention for the Protection of Human Rights and Fundamental Freedoms, 4 November 1950.

[2] Charter of Fundamental Rights of the European Union, OJ C 202/2, 7.6.2016, p. 389-405.

[3] Article 8 (1) of the European Convention on Human Rights.

[4] Article 7 of the Charter of Fundamental Rights of the European Union.

[5] European Court of Human Rights, *Costello-Roberts v. the United Kingdom,* Judgement of 25 March 1993, no. 13134/87, para. 36.

[6] European Court of Human Rights, *Von Hannover v. Germany (no. 2)*, Judgement of 7 February 2012, para. 95.

[7] European Court of Human Rights, *Airey v. Ireland*, Judgement of 9 October 1979, no. 6289/73, para. 32 and *Z. and Others v. the United Kingdom*, Judgement of 10 May 2001, no.29392/95, para. 74.

Finally, Article 52 (3) of the CFREU states that *"in so far as this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention"*. When both the ECHR and the CFREU contain corresponding rights, such as the right to privacy, the CJEU should follow the interpretation of the ECtHR.

2.1.1.2 An interference with the right to privacy

Once the existence of an interference with the right to privacy has been determined, it must be assessed whether or not this interference is also a violation, and thus not justified.

Article 8 (2) of the ECHR establishes a three-step test which requires that an interference is: (1) in accordance with the law, (2) necessary in a democratic society, and (3) in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

The CFREU takes a very similar approach in article 52 by stating that any limitation must: (1) be provided for by law, (2) respect the essence of those rights and freedoms, (3) be necessary, (4) genuinely meet objectives of general interest recognized by the Union or the need to protect the rights and freedoms of others.

The current analysis will look at those elements which are common to both legal instruments. First of all, the interference must be in accordance with the law. This condition requires the existence of a national law that is sufficiently clear, foreseeable, and adequately accessible. This means that the law must be sufficiently clear, precise, and detailed in its formulation as to enable a citizen to regulate his/her own conduct and reasonably foresee the consequences of his/her actions. Additionally, the citizen must be able to access the law and have an indication that it is applicable in the relevant situation.[8]

Secondly, the interference must have a legitimate aim. Article 8 (2) of the ECHR gives an exhaustive list of possible grounds which, if applicable, qualify as legitimate aims. In contrast, article 52 of the CFREU takes a more open approach, which allows for any objective of general interest recognized by the Union to qualify as a legitimate aim. It also includes the need to protect the rights and freedoms of others as a possible legitimate aim.

Lastly, the interference must be proportional to the legitimate aims pursued. The ECHR refers to the concept of proportionality by stating that the interference must be 'necessary in a democratic society', while the CFREU mentions the condition of necessity together with proportionality. In any case, the ECtHR has said that necessity refers to a 'pressing social need'[9], and not to mere 'usefulness' or 'desirability'.[10] The measures behind the interference must also be relevant and sufficient, while being proportional to the legitimate aim.[11] This means that the interference must be able to achieve the legitimate aim while there is an absence of less intrusive alternatives to achieve the same results.

2.1.2 The right to data protection

Both privacy and data protection are closely related concepts and the scope of these fundamental rights overlaps to a certain extent. The right to data protection aims to protect the personal data of individuals, while the right to privacy protects one's private life. An infringement of one of these rights

[8] European Court of Human Rights, *Silver and Others v. the United Kingdom,* Judgement of 25 March 1983, para. 86-88.

[9] It is a duty of the respondent state to demonstrate this 'pressing social need'.

[10] European Court of Human Rights, *Dudgeon v. The United Kingdom*, Judgement of 22 October 1981, no. 7525/76, para. 51.

[11] European Court of Human Rights, *Z v. Finland*, Judgement of 25 February 1997, no. 22009/93, para. 94.

does not automatically lead to an infringement of the other right. For example, the right to data protection will not be triggered if a case does not involve the processing of any personal data, while there may still exist an infringement in the individual's private life.

Although the ECtHR has recognized the right to data protection, it is not explicitly mentioned in the ECHR. In *S and Marper v. the United Kingdom,* the Court acknowledged this right as being part of the right to privacy by stating that: "*the protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life as guaranteed by article 8 ECHR*".[12] Following this acknowledgement, the Court has developed several general principles of data protection in its case law. For example, in the *Leander v. Sweden* case, the Court held that the storing and releasing of information relating to the private life of an individual by a public authority amounts to an interference with the right to privacy.[13]

The CJEU already recognized the right to protection of personal information as a general principle of EU law in 1969.[14] With the adoption of the CFREU, the right to data protection has also been made explicit as a separate fundamental right. Article 8 of the CFREU makes clear that "*everyone has the right to the protection of personal data concerning him or her"* and also sets out specific conditions concerning the processing of personal data. These conditions already hint to some of the data protection principles and concepts found in secondary legislation, such as the GDPR. In order not to infringe upon article 8 of the CFREU, the personal data must be "*processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law."* . It also states that "*everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.".*[15]

In order for an infringement with the right to data protection to be justified, it must satisfy the requirements of article 8 (2) of the ECHR and article 52 of the CFREU. These will not be explained further, since a brief analysis of these requirements has already been provided in the previous section. The main difference with the right to privacy is the addition of the conditions found in article 8 (2) of the CFREU, as mentioned in the previous paragraph.

The specific relationship between the fundamental rights to privacy and data protection will be further explored in D7.2.

2.2 The General Data Protection Regulation

This chapter will identify the legal framework applicable to KRAKEN in relation to the processing of personal data. First, the scope of application and definitions will be discussed in order to determine how the GDPR applies to the KRAKEN project. Secondly, the data protection principles, legal grounds, security of processing, and data subject rights will be discussed considering they give rise to important obligations for the controller and processor.

2.2.1 Scope and definitions

The entry into force of the GDPR on 25 May 2018 marked a new era in the world of data processing. The purpose of the GDPR is to protect natural persons with regard to the processing of their personal data while still ensuring the free movement of such data.[16] In this sense, the Regulation aims to protect

[12] European Court of Human Rights, *S and Marper v. the United Kingdom*, Judgement of 25 August 1997, no. 20837/92, para. 103.

[13] European Court of Human Rights, *Leander v. Sweden*, Judgement of 26 March 1987, no. 9248/81, para. 48.

[14] Court of Justice of the European Union, *Stauder*, Judgement of 12 November 1969, C-29/69.

[15] Article 8 (2) of the Charter of Fundamental Rights of the European Union.

[16] Article 1 of the GDPR.

individuals by giving them control over their personal data and through placing responsibilities on data controllers in a way which is compatible with the European Single Market.

2.2.1.1 The 'processing' of 'personal data'

Article 2 of the GDPR determines that the Regulation applies to *the* ***processing*** *of* ***personal data.*** The GDPR defines these terms in Article 4 (1) and (2):

> *"**'personal data'** means <u>any information relating to an identified or identifiable natural person</u> ('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."*[17]
>
> *"**'processing'** means <u>any operation or set of operations which is performed on personal data or on sets of personal data</u>, 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."*[18]

From this definition we can conclude that the concept of ***processing*** is quite broad. It applies to the entire data lifecycle (from collection to destruction) and is not limited to a specific type of operation.

The definition of ***personal data*** requires a bit more clarification. It starts by stating that *any information* could qualify as personal data, as long as that information *relates to an identified or identifiable natural person* (i.e. the data subject). This means that the specific type of content or format of that information is irrelevant for its qualification as personal data. It goes on to state that, by making use of so-called identifiers, identification can occur either directly from the information, or indirectly from the information in combination with additional information. The definition provides several examples of identifiers, in addition to Recital 30, which also mentions internet protocol addresses, cookie identifiers, and even radio frequency identification tags as possible identifiers.

The question still remains, when is a natural person considered to be *identifiable*? Recital 26 of the GDPR provides some clarity with regard to the concept of *identifiability*:

> *"To determine whether a natural person is identifiable, account should be taken of <u>all the means reasonably likely to be used</u>, such as singling out, <u>either by the controller or by another person to identify the natural person directly or indirectly.</u> To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments."*[19]

In order to determine whether or not an individual is *identifiable*, we have to consider *all the means reasonably likely to be used* to identify that individual. On first sight, this might be a difficult and subjective assessment to make. However, the GDPR explicitly states that all objective factors should be taken into account (e.g. cost and time for identification, available resources, state of the art, etc.). If, on the basis of these objective factors, it is reasonably likely that certain means could be used to identify a natural person, then the applicability of the GDPR will be triggered. It is also important to

[17] Article 4 (1) of the GDPR.
[18] Article 4 (2) of the GDPR.
[19] Recital 26 of the GDPR.

note that these means of identification can be used by *either the controller or by another person.* It is therefore important to not only consider the perspective of the controller, but rather the perspective of any person that could identify the individual in question. In case the GDPR applies to certain processing activities on personal data, then the controller and processor must respect the data protection principles and comply with the obligations contained in the GDPR.

2.2.1.2 Anonymization and pseudonymization

Next, we arrive at two important concepts for the scope of application of the GDPR, namely ***anonymization*** and ***pseudonymization***. The GDPR defines these terms in Recital 26 and Article 4 (5):

> ***'anonymization'*** refers to "*information which does not relate 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.*"[20]
>
> "***'pseudonymization'*** *means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person*"[21]

It is clear from these definitions that there exists a crucial difference between anonymized and pseudonymized data with regard to the applicability of the GDPR. In short, anonymized data does not relate to an identified or identifiable natural person, and therefore does not fall under the scope of the GDPR.[22] It is necessary that the employed anonymization technique is irreversible, taking into account *all the means reasonably likely to be used* to re-identify the individual. All parties, including third-parties, should be unable to single out an individual in a dataset, link two record within or between datasets, or infer personal information in a dataset.[23] It must be noted that the act of anonymizing data is considered a processing activity in itself. Consequently, the GDPR will apply to the processing of personal data up until the data has been fully anonymized, including the act of anonymization. This also means that, as a processing activity, anonymization must rely on a legitimate legal basis[24] in order to comply with the GDPR. There are several options in this regard, such as; consent, the legitimate interests of the controller, and compliance with a legal obligation. The GDPR also mentions that if a controller no longer requires identification of a data subject for its processing purposes, the controller is not obliged to maintain, acquire, or process additional information for the identification of the data subject.[25] Lastly, even if the GDPR does no longer apply, anonymized data may still fall under other legal frameworks (e.g. the fundamental right to privacy and the ePrivacy framework).[26]

Pseudonymized data, on the other hand, still falls under the legal regime of data protection. According to the definition, pseudonymized data can still be attributed to an individual with the use of additional information. As long as an individual can still be re-identified by any party, with the use of additional information (*by means reasonably likely to be used)*, the personal data is in fact pseudonymized rather than anonymized. From a legal point of view, the threshold for 'full anonymization' is therefore quite

[20] Recital 26 of the GDPR.

[21] Article 4 (5) of the GDPR.

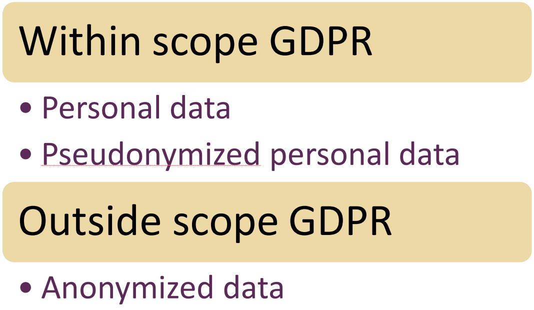
[22] Recital 26 of the GDPR.

[23] Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymization Techniques, 10 April 2014, 0829/14/EN WP216, 9.

[24] List of legal bases under article 6 and 9 of the GDPR, which will be discussed in section 2.2.3 and 2.2.4.

[25] Article 11 of the GDPR.

[26] Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymization Techniques, 10 April 2014, 0829/14/EN WP216, 11.



Within scope GDPR

- Personal data
- Pseudonymized personal data

Outside scope GDPR

- Anonymized data

Figure 1.1 Anonymized and pseudonymized data

high and difficult to attain. Even though pseudonymization does not remove personal data from the scope of the GDPR, it is still a useful technical measure and safeguard that can contribute to compliance with the data protection principles and the GDPR as a whole.[27]

The CJEU has dealt with the question of identifiability and pseudonymization before. In the *Patrick Breyer* case, the Court was asked whether a dynamic IP address constitutes personal data, considering it cannot be attributed to a natural person without the use of additional information. The question then becomes one of identifiability, and whether this additional information can be acquired by *all the means reasonably likely to be used*. The Court was of the opinion that:

> *"a dynamic IP address registered by an online media services provider when a person accesses a website that the provider makes accessible to the public constitutes personal data within the meaning of that provision, in relation to that provider, where the latter has the legal means which enable it to identify the data subject with additional data which the internet service provider has about that person."*[28]

This judgement follows the approach of the GDPR regarding identifiability. If the additional information (e.g. a decryption key) can be obtained by lawful means reasonably likely to be used (e.g. legal means), then the data in question (e.g. a dynamic IP address) constitutes personal data, which will trigger the applicability of the GDPR.

2.2.1.3 'Controller' and 'processor'

The GDPR aims to protect individuals by giving back control over their data and by holding the data ***controller*** legally responsible and accountable. Article 4 (7) of the GDPR defines this term as:

> *"'**controller**' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, <u>determines the purposes and means of the processing of personal data</u>; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law"*[29]

The crucial element for the qualification as a controller is that an entity must *determine the purposes and means of the processing of personal data.* First of all, the controller must have a factual influence over the processing activities through some type of decision-making power. This factual control can be derived from an explicit legal competence (e.g. explicitly laid down in Union or Member State law) or an implicit competence (e.g. implicitly derived from an assigned task). In case there is no clear explicit

[27] Recital 28 of the GDPR.

[28] Court of Justice of the European Union, *Patrick Breyer v. Bundesrepublik Deutschland*, Judgement of 19 October 2016, C-582/14, para. 49.

[29] Article 4 (7) of the GDPR.

or implicit competence, only a factual assessment of the circumstances and processing activities can reveal the responsible controller(s). Secondly, this factual control of the controller manifests itself by determining the purposes (the 'why') and means (the 'how') of the processing activities. There is a certain level of detail to which an entity should determine the purposes and means in order to be considered a controller. Regarding the means of processing (e.g. technical and organizational measures), an entity must decide on the essential elements, such as; the types of data, data subjects, retention periods, access rights, recipients of the data, etc. The non-essential elements (e.g. specific hardware or software to be used) could, in principle, be determined by the data processor. It is also not necessary that the controller has direct access to the personal data.[30]

This brings us to the concept of data ***processor***, as defined in Article 4 (8) of the GDPR:

> *"'**processor**' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller"*[31]

As opposed to the role of controller, the processor does not determine the purposes (the 'why') and the means (the 'how') of processing, but rather processes personal data on behalf of the controller. The processor carries out a specific task and follows a set of instructions determined by the controller in relation to the purposes and essential elements of the means. Depending on the specific instructions of the controller, the processor can enjoy a certain degree of autonomy with regard to the non-essential elements of processing. In practice, the mandate and modalities of the processor will be laid down in a data processing agreement between the controller and processor, as stated in Article 28 (3) of the GDPR. In any case, the controller must ensure that the processor provides sufficient guarantees to implement appropriate technical and organizational measures in order to satisfy the requirements and obligations of the GDPR.[32] It is possible that a processor infringes upon the data processing agreement by acting beyond the specified mandate. When a processor starts determining the purposes and essential elements of the means of processing, taking into account the factual circumstances, its qualification may change to the role of a controller (or joint controller).[33]

It is also possible that two or more controllers jointly determine the purposes and means of processing, in which case they are considered to be joint controllers. In this scenario, both controllers must, in a transparent manner, determine their respective responsibilities for compliance with their obligations under the GDPR. It is particularly important that both controllers make clear arrangements regarding the exercise of the rights of data subjects and their respective duties.[34] The CJEU has provided some clarity on the concept of joint controllership in its case law, namely in the *Wirtschaftsakademie*[35] and *Fashion ID*[36] cases.

[30] European Data Protection Supervisor, Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725, 7 November 2019, 7 – 10.

[31] Article 4 (8) of the GDPR.

[32] Article 28 (1) of the GDPR.

[33] European Data Protection Supervisor, Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725, 7 November 2019, 16 - 17.

[34] Article 26 of the GDPR.

[35] Court of Justice of the European Union, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH,* Judgement of 5 June 2018, C-210/16; for a more in-depth analysis of this case, see SCHROERS, J., The Wirtschaftsakademie case: Joint Controllership, 2018, available at https://www.law.kuleuven.be/citip/blog/the-wirtschaftsakademie-case-joint-controllership/.

[36] Court of Justice of the European Union, *Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV,* Judgement of 29 July 2019, C-40/17; for a more in-depth analysis of this case, see CHRISTOFI, A., The Fashion ID judgement: broad definition of (joint) controllership solidified, 2019, available at https://www.law.kuleuven.be/citip/blog/the-fashion-id-judgment-broad-definition-of-joint-controllership-solidified/.

In the first case, Wirtschaftsakademie hosted an educational fan page on Facebook. However, none of the parties involved informed visitors that their personal data was being collected via cookies. Wirtschaftsakademie was of the opinion that it was not a data controller since it had no factual or legal control over the purposes and means of processing. Several questions were referred to the CJEU, two of which were relevant for the concept of joint controllership: 1) can there be responsibility for an entity which is not a controller? and 2) can it be said that in case an entity is not a controller, this entity does not have the obligation of choosing a processor?

The CJEU held that the data controller plays a fundamental role as the responsible entity for compliance with the data protection framework. The concept of controllership must be interpreted based on a factual analysis and must be given a broad interpretation in order to ensure effective and complete protection of data subjects. Such a factual analysis must take into account who in reality determines the purposes and means of processing. In this case, the goal of Facebook was to improve its advertising system through the creation of fan pages by users. Wirtschaftsakademie, on the other hand, provided the target demographic for that goal. For these reasons, Facebook and Wirtschaftsakademie should be considered to be joint controllers. It is, however, not necessary that all joint controllers share the same degree of responsibility in the processing activities.

In the second case, Fashion ID embedded a Facebook 'Like' button on their online shop. As a result, personal data from the visitor's browser was transmitted to Facebook Ireland. This transmission of data occurred regardless of whether the visitor was a member of social network Facebook or had clicked on the Facebook 'Like' button. Fashion ID argued that it was not a data controller since it had no control over the transmission of data to Facebook Ireland, and how Facebook Ireland would process that data. Again, the CJEU was asked several questions, some of which are relevant: 1) is Fashion ID a controller, by the fact that it has embedded a plugin (the Facebook 'Like' button) on its website that enabled the transmission of personal data to a third party? and 2) should Fashion ID or the plugin-provider (Facebook Ireland) obtain consent from visitors and inform them about the data processing?

The Court held that Fashion ID was aware of the fact that the plugin, made available by Facebook Ireland, served as a tool for data collection and disclosure of visitor's personal data, regardless of whether visitors were members of the social network Facebook. By doing this, Fashion ID exercised decisive control over, and (implicitly) consented to, the collection and transmission of visitor's personal data to Facebook Ireland, which could not have occurred without such a plugin. As a result, Fashion ID enjoyed a commercial advantage by embedding the plugin on its website and the processing activities were therefore in the economic interest of both Fashion ID and Facebook Ireland. Consequently, it appears that both parties jointly determined the purposes of the collection and transmission of personal data. In the end, the Court dismissed the argument that Fashion ID had no access to the data collected and transmitted to Facebook Ireland, or that Fashion ID had no control over the data transmitted and how Facebook Ireland would process that data.

2.2.2 Data protection principles

The GDPR establishes a set of core data protection principles that must be respected throughout the entire data processing lifecycle.[37] In many cases, these principles correspond to obligations of the controller and rights of the data subject. In this sense, they encompass the application of the GDPR in its totality.

2.2.2.1 Lawfulness, fairness and transparency

According to Article 5 (1) (a) of the GDPR, personal data should be "*processed lawfully, fairly and in a transparent manner in relation to the data subject*". The principles of lawfulness, fairness and

[37] Article 5 of the GDPR.

transparency guarantee that data will be processed in accordance with the law, proportionally to the aim foreseen and with transparent means for the data subject who must be informed about the processing of their personal data.

The principle of **lawfulness** imposes that all processing activities must comply with the law and must rely on a legitimate legal basis[38], which implies not only data protection legislation but also other types of legislation that could apply to a specific sector (e.g. financial legislation, energy legislation, etc.).

The principle of **fairness** introduces a balancing test that has to be carried out for each processing activity, since the right to the protection of personal data must be balanced with other potentially conflicting rights and interests (e.g. freedom of information, public security, etc.). This balance can be achieved through strict compliance with the general data protection principles and ensuring respect for data subject rights by the controller. In essence, personal data must not be processed in a way which unreasonably infringes the fundamental right to the protection of personal data of the data subject. As a result, processing can be lawful but still considered unfair in respect of the means foreseen and the reasonable expectations of the data subject. Consequently, it is essential that processing activities are always clear to the data subject and that he/she is aware of his/her rights under the GDPR.[39]

As a core data protection principle, **transparency** applies to all stages of the processing lifecycle; i.e. before data collection, at the moment of data collection, during subsequent processing activities, during communications with the data subject, in case data processing modalities change, etc. Article 12 of the GDPR makes clear that all information (related to Article 13 and 14) and communications (under Articles 15 to 22 and 34) on the processing of personal data should be provided to the data subject in a concise, transparent, intelligible, and easily accessible form, while using clear and plain language.[40] The aim is to ensure that data subjects are exhaustively aware of the processing activities and extent of processing relating to their personal data.[41] Consequently, the principle of transparency is closely linked to the information obligations[42] and data subject rights[43] provided by the GDPR.

2.2.2.2 Purpose limitation

The principle of **purpose limitation** states that personal data may only be collected for "*specified, explicit and legitimate purposes*" and "*not further processed in a manner that is incompatible with those purposes*".[44] Personal data may only be collected if the controller knows how, when, and why the data will be processed. The controller should therefore determine the purposes of processing well before any processing activity takes place (incl. the collection of personal data).

Firstly, the purposes should be sufficiently specific and not merely based on broad or vague concepts (e.g. business interests, IT system security, future research, etc.). Secondly, the specified purposes must be explicit, which means that the controller must provide a clear and intelligible description of the purposes to the data subject. In this way, the requirement of explicitness is closely related to the principle of transparency. The aim is to avoid vagueness or ambiguity in the specification and description of the purposes and to ensure that the data subject fully understands the meaning and intent behind the purposes. This does not imply that longer and overly detailed explanations are necessary, as they might be counter-productive. Thus, the level of detail which is required to properly

[38] Article 6 of the GDPR.

[39] D., Clifford and J., Ausloos, Data Protection and the Role of Fairness, KU Leuven Centre for IT & IP Law, CiTiP Working Paper 29/2017, 3 August 2017, 11 – 20.

[40] Article 12 and Recital 58 of the GDPR.

[41] Recital 39 of the GDPR.

[42] Articles 13 and 14 of the GDPR.

[43] Articles 15 to 22 of the GDPR.

[44] Article 5 (1) (b) of the GDPR.

inform the data subject may differ depending on the context and complexity of processing activities. A layered approach is often suggested; essential information is provided in a concise and clear way, while additional information and details are provided via a secondary channel (e.g. a website link) in case clarifications are required.[45] Finally, the specific purposes must also be legitimate and thus in accordance with the law. The interpretation of 'law' is quite broad, referring not only to applicable data protection legislation, but rather all forms of written and common law, primary and secondary legislation, municipal decrees, fundamental rights, legal principles, jurisprudence, etc.[46]

Article 5 (1) (b) of the GDPR also mentions that personal data may '*not be further processed in a manner that is incompatible with those purposes*'. Processing activities following the collection of personal data must be limited to the specified purposes or to a purpose that is compatible with the initial purposes. This compatibility test must be assessed on a case-by-case basis, taking into account several factors, such as; any link between the initial purpose and the new purpose, the context in which the personal data have been collected (e.g. the relationship between data subject and controller), the nature of the personal data, the potential effects of further processing for data subjects, and the implementation of safeguards to protect the data subject.[47] In case the initial and new purposes are deemed compatible, no new legal basis other than the original legal basis (i.e. the legal basis that allows for the processing for the initial purpose) is required.[48] Lastly, the purpose limitation principle also states that *'further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89 (1), not be considered to be incompatible with the initial purposes."*[49] This last part creates a presumption of compatibility for archiving, scientific, historical, and statistical purposes. It must be noted that, although the purposes should be considered to be compatible, the presumption of compatibility is not a free pass for further processing and each case must still be assessed in its own context, taking into account appropriate safeguards and measures.[50]

2.2.2.3 Data minimization and storage limitation

According to the principle of **data minimization**, personal data must be "*adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed*".[51] In essence, this principle asks whether the same purpose can be achieved with a more limited collection of personal data. The principle of data minimization is intrinsically linked to the purpose limitation principle, since it is an application of the principle of proportionality in relation to the specified purposes. It is particularly important for the concept of data protection by design and by default, as it is explicitly mentioned in Article 25 of the GDPR. In order to effectively apply the principle of data minimization, it is important that organizations periodically review processing activities to check whether the personal data they hold is still adequate, relevant, and limited to what is necessary for the specified purposes. If this is not the case, unnecessary personal data should be deleted and incorrect or incomplete data should be rectified.

This brings us to the **storage limitation** principle, which is closely linked to the principles of data minimization and purpose limitation. It states that personal data must be "*kept in a form which permits*

[45] Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, 2 April 2013, 00569/13/EN, WP203, 16 – 17.
[46] Ibid., 20.
[47] Article 6 (4) of the GDPR.
[48] Recital 50 of the GDPR.
[49] Article 5 (1) (b) of the GDPR.
[50] European Data Protection Supervisor, A preliminary Opinion on data protection and scientific research, 6 January 2020, 22.
[51] Article 5 (1) (c) of the GDPR.

identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;".[52] This implies that personal data must either be removed or irreversibly de-identified when they are no longer necessary for the specified purposes. It is thus advised that organizations, in addition to periodic reviews, establish storage, retention, and deletion policies prior to the collection of personal data. The storage limitation principle also allows for longer storage periods for processing solely for archiving, scientific, historical, and statistical purposes, under the condition that appropriate technical and organizations measures are implemented to protect the data subject.[53]

2.2.2.4 Accuracy

According to the principle of **accuracy**, personal data should be "*accurate and, where necessary, kept up to date".*[54] The controller must ensure accuracy at all stages of the processing lifecycle, taking every reasonable step to erase or rectify inaccurate personal data without delay. This can be achieved through review mechanisms and a proper exercise of the data subject's right to rectification and erasure.

2.2.2.5 Integrity and confidentiality

In addition to keeping personal data accurate and up-to-date, the controller must also ensure the **integrity and confidentiality** of personal data. Personal data must be processed "*in a manner that ensures appropriate security of personal data*".[55] The aim is to protect personal data against unauthorized or unlawful processing, accidental loss, destruction, or damage. This can be achieved by implementing appropriate technical or organizational measures, such as clearly defined access policies, systemic quality controls, and technical features against data breaches. The level of security should also be periodically reviewed to ensure constant protection of personal data.

2.2.2.6 Accountability

Lastly, the GDPR explicitly establishes the principle of **accountability** by stating that the "*controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1."*[56] Paragraph 1 in this sentence refers to the other data protection principles discussed above.

In essence, the controller is responsible for actively implementing appropriate technical and organizational measures in order to promote and safeguard the protection of the personal data and to be able to demonstrate that processing activities are conducted in accordance with the GDPR.[57] In this context, the controller is obliged to keep records of processing activities under its responsibility in order to promote and demonstrate compliance.[58] This also applies to the legal basis of consent, which the controller should also be able to demonstrate.[59] For these reasons, it is important for organizations to implement record-keeping systems for possible audits and inspections. Specific tools, such as a dynamic consent management tool, can greatly contribute towards the principle of accountability by providing clear evidence of valid consent and accompanying processing activities.

[52] Article 5 (1) (e) of the GDPR.
[53] Ibid.
[54] Article 5 (1) (d) of the GDPR.
[55] Article 5 (1) (f) of the GDPR.
[56] Article 5 (2) of the GDPR.
[57] Article 24 of the GDPR.
[58] Article 30 of the GDPR.
[59] Article 7 (1) of the GDPR.

2.2.3 Legal basis for processing

The data protection principle of 'lawfulness' makes clear that the processing of personal data must be based on, and limited to, a legal ground. Article 6 of the GDPR provides six possible legal grounds on which a controller can rely for its processing activities. Because not every legal ground found in Article 6 is relevant for KRAKEN, this section will only discuss the legal grounds of (1) consent[60], (2) necessary for the performance of a contract[61], (3) necessary for compliance with a legal obligation[62], (4) necessary for the performance of a task carried out in the public interest[63], and (5) necessary for the legitimate interest of the controller or a third party[64].

It should also be noted that the data protection principles discussed in the previous section are closely linked to the legal grounds. The extent of their application is influenced by the choice and modalities of the applicable legal ground. For example, the extent of the data minimization principle will depend on the modalities of consent or the applicable legal obligation.

2.2.3.1 Consent

Consent is the first, and most well-known, possible legal basis for the processing of personal data.[65] In order to obtain valid consent from the data subject, it must be *(a) freely given, (b) specific, (c) informed,* and *(d) unambiguous*:

> *(a) freely given:* the data subject must have a genuine and free choice; there should be no imbalance of power.
>
> *(b) specific*: consent should cover all processing activities carried out for the same purpose and separate consent should be given for each purpose.
>
> *(c) informed:* the data subject must be properly informed in an intelligible way, using clear and plain language.
>
> *(d) unambiguou*s: consent must constitute a clear affirmative action and must show an unambiguous indication of the data subject's wishes; silence, pre-ticked boxes, or inactivity do not constitute consent.[66]

Additionally, the request for consent must be clearly distinguishable as such and it must be provided in an intelligible and easily accessible form, using clear and plain language. The controller must be able to demonstrate that the data subject has given valid consent and it must be made clear to the data subject that consent can be withdrawn at any time without any detrimental effects.[67] Due to the strict criteria for validity and the ability of the data subject to withdraw consent, it may not always be the most desirable legal ground. Rather, consent should ideally be relied on when other legal grounds are not viable.

In the case of an online marketplace, which can be qualified as an '*information society service'*[68]*,* additional conditions apply when consent is obtained from a child. When an information society

[60] Article 6 (1) (a) of the GDPR.

[61] Article 6 (1) (b) of the GDPR.

[62] Article 6 (1) (c) of the GDPR.

[63] Article 6 (1) (e) of the GDPR.

[64] Article 6 (1) (f) of the GDPR.

[65] Article 6 (a) of the GDPR.

[66] Article 4 (11) and Recital 32 of the GDPR; European Data Protection Board, Guidelines 05/2020 on consent Under Regulation 2016/679, 4 May 2020, 7 – 19.

[67] Article 4 (11), 7, and Recital 32 of the GDPR.

[68] Defined as "*any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services*" by Article 1 (1) (b) of Directive (EU) 2015/1535 of the European

service is directly offered to a child, consent shall only be lawful where the child is at least 13 to 16 years old, depending on the Member State. If the child is younger, consent must be given or authorized by the holder of parental responsibility over that child.[69] [70]

2.2.3.2 Necessary for the performance of a contract

The legal grounds other than consent all require the condition of *necessity*. In order for a processing activity to be lawful under these legal grounds, they must be necessary for the specific purpose of that legal ground (i.e. performance of a contract, compliance with a legal obligation, performance of a task carried out in the public interest, and legitimate interest of the controller). Following a fact-based assessment, necessity implies that the processing activity is effective in reaching its objective and is the least intrusive option available.[71]

The second legal ground under Article 6 is the processing of personal data in case 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 the contract.[72] This may be the case when a data subject orders goods or services online and the company processes contact details in order to perform the contract. This legal basis could also apply to KRAKEN when it is necessary for the user to create an account in order to transact data on the platform. The processing of personal data that is required to create an account (e.g. an e-mail address), and therefore to transact data on the platform, can be considered necessary to provide the service.

In any case, the processing activity cannot be considered *necessary* if there exists an alternative method of performing the contract without intrusive processing of personal data or if it is considered merely useful rather than necessary.

2.2.3.3 Necessary for compliance with a legal obligation or for the performance of a task carried out in the public interest

It may also be necessary for a controller to process personal data in order to comply with a **legal obligation**.[73] This applies to controllers from both the private and public sector, such as; a bar association, a chamber of medical professionals, a municipal authority, a local swimming pool, etc.[74] [75] 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 ground. This can be done by laying down specific requirements and measures to ensure lawful and fair processing of personal data.[76] The Union or Member State law that provides for the legal ground must be sufficiently clear and must determine the purpose of processing. It may further specify general conditions of processing, the types of data, the data subjects, storage periods, etc. The law must also meet an objective of public interest and must be proportionate to the

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.

[69] Article 8 of the GDPR.

[70] Article 29 Data Protection Working Party, Guidelines on consent under Regulation 2016/679, 28 November 2017 and last revised and adopted on 10 April 2018, 17/EN, WP259 rev.01, 23 – 24.

[71] 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, 9 April 2019, 7.

[72] Article 6 (b) of the GDPR.

[73] Article 6 (c) of the GDPR.

[74] 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.

[75] 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.

[76] Article 6 (2) of the GDPR.

aim pursued.[77] Finally, the processing of personal data in the context of a legal obligation may not be voluntary for the controller.[78] This legal obligation may arise from many different legal frameworks, such as financial legislation (e.g. 'know your customer (KYC)' obligations) or fiscal legislation (e.g. employee salary data to social security or tax authorities).[79]

The previous analysis also applies to the processing of personal data necessary for the performance of a **task carried out in the public interest or in the exercise of official authority** vested in the controller.[80] However, in this case the controller is not under any requirement to act under a legal obligation and processing activities under this legal ground may be voluntary.[81]

2.2.3.4 Necessary for the legitimate interests of the controller or a third party

The processing of personal data is also lawful if it meets the conditions of Article 6 (f) of the GDPR. Firstly, there must exist a legitimate interest pursued by the controller or a third party. This legitimate interest may be legal, economic, or non-material in nature, and must relate to a real and present issue (e.g. to protect against vandalism or to prevent fraud).[82] Secondly, as mentioned before, the processing of personal data should be limited to what is adequate, relevant, and *necessary* for the specified purposes. Processing may only take place if other less intrusive measures cannot reasonably fulfill the purposes of processing. Lastly, in order to rely on this legal ground, it is mandatory to perform a balancing test of the interests of the parties involved. The controller may 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.[83] The controller must assess the effects and potential negative consequences of the processing activities on the interest and fundamental rights and freedoms of the data subject. This balancing exercise must be conducted on a case-by-case basis, taking into account the specific factors and circumstances of the situation.[84] The intensity of the intervention (f.e. the type of personal data, the number of data subjects, the scope of processing, existing alternative options, etc.) is considered the most important factor in this balancing exercise. Another important element, according to Recital 47 of the GDPR, are the reasonable expectations of the data subject at the time and in the context of the collection of personal data. This should be determined from the point of view of an objective third party and whether or not this third party could reasonably expect that its personal data could be processed in said situation.

The legal ground of legitimate interests cannot be invoked by public authorities in the performance of their tasks.[85]

2.2.4 Special categories of personal data

Some categories of personal data receive special treatment under the GDPR, such as increased security measures, due to their highly sensitive nature and increased processing risks. These risks should be taken into account when determining the appropriate level of security for these special categories of

[77] Article 6 (3) of the GDPR.
[78] 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.
[79] Ibid.
[80] Article 6 (e) of the GDPR.
[81] 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.
[82] Ibid., 24.
[83] Article 6 (f) of the GDPR.
[84] 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.
[85] Article 6 (1) of the GDPR.

personal data (i.e. sensitive personal data).[86] 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.[87] Exceptionally, the processing of these special categories of personal data is allowed if it falls under one of the special legal grounds of Article 9 of the GDPR. These special legal grounds must always be applied cumulatively with one of the general legal grounds of Article 6.

In particular, the processing of these special categories of personal data is allowed when the data subject has given **explicit consent** to the processing of those personal data for one or more specified purposes. It is, however, possible that Union or Member State law provides that the data subject may not consent to the processing of these special categories of personal data.[88] The basic conditions for explicit consent are the same as for 'normal' consent. The term 'explicit' refers to the manner in which consent is expressed by the data subject. More specifically, the data subject must give an express statement of consent, such as a written statement on paper, on an electronic form, or even in an e-mail. In principle, an express oral statement may also suffice, but this can prove problematic for the controller with regard to providing evidence of valid consent.[89]

In total, there are ten special legal grounds for the processing of special categories of personal data. Some of them are similar to the general legal grounds of Article 6, such as the processing necessary for reasons of substantial public interest.[90] However, most of the special legal grounds pertain to very specific situations, such as the processing necessary for the purposes of carrying out obligations in the field of employment and social security, or the processing necessary for the establishment, exercise or defence of legal claims.[91]

Finally, Member States are allowed to maintain or introduce further conditions, including limitations, regarding the processing of *genetic data, biometric data,* or *data concerning health.*[92] For these types of sensitive data, it is also important to look at national legislation in order to identify additional limitations.

2.2.5 Security of processing

Following the risk-based approach adopted by the GDPR, the level of security assigned to certain types of personal data or processing activities varies depending on the accompanying risks for the data subject. According to Article 24 of the GDPR, the controller must implement appropriate technical and organizational measures to ensure and to be able to demonstrate that its processing activities are GDPR compliant.[93] This risk-based approach and obligation to implement appropriate technical and organizational measures is reiterated in Article 32 of the GDPR, which obliges the controller and the

[86] Article 32 (2) of the GDPR.

[87] Article 9 (1) of the GDPR.

[88] Article 9 (2) (a) of the GDPR.

[89] European Data Protection Board, Guidelines 05/2020 on consent Under Regulation 2016/679, 4 May 2020, 20 – 21.

[90] Article 9 (2) (g) of the GDPR.

[91] Article 9 (2) (b) and (f) of the GDPR.

[92] Article 9 (4) of the GDPR.

[93] The controller must "*take 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*".

processor to ensure a level of security appropriate to the risk.[94] Potential appropriate measures include: (a) the pseudonymization and encryption of personal data, (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services, (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident, and (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.[95] When assessing the appropriate level of security, the controller and processor should take into account the risks of processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed.[96]

In general, organizational measures relate to enforcing proper management frameworks, procedures, and policies (e.g. 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 (e.g. cybersecurity measures, physical protection, encryption, access rights, authentication and authorization measures, system restoration, etc.). An initial description of the project's organizational and technical measures can be found in Deliverable 8.6.

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.[97] It is clear that data protection by design and security by design are not mutually exclusive concepts and furthermore contribute to each other.

2.2.6 Data subject rights

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 the corresponding responsibilities and obligations of data controllers and processors. As a result, the controller must be organizationally prepared for requests pertaining to data subject rights, for example by providing a contact point, portal, or access to information.

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

The use of blockchain technology can also create tensions with regard to the exercise of data subject rights, especially when this technology makes it difficult to identify the controller (e.g. on a public, permissionless blockchain). The main obstacle exists in the immutability of the blockchain, which makes it difficult or even impossible to erase or update data on a node in the chain. It is, however, possible to achieve similar effects by using other techniques than erasure (e.g. encryption and key destruction).[98]

[94] The controller and processor must "*take into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons*".

[95] Article 32 (1) of the GDPR.

[96] Article 32 (2) of the GDPR.

[97] Article 25 (1) of the GDPR.

[98] The European Union Blockchain Observatory and Forum, Thematic Report on Blockchain and the GDPR, 2018, 25 – 26.

2.2.6.1 Right to information

According to Articles 13 and 14 of the GDPR, the controller must provide the data subject with the following information: (1) the identity and contact details of the controller, (2) where applicable, the contact details of the data protection officer (DPO), (3) the purposes of processing as well as the legal basis for processing, (4) where applicable, the legitimate interests of the controller or third party, (5) the categories of personal data, (6) the recipients of the personal data, (7) in case of an international transfer of personal data, the existence of an adequacy decision by the Commission or reference to appropriate and suitable safeguards.[99]

Additionally, in order to ensure fair and transparent processing, the controller must also provide the data subject with information on: (1) the storage period or criteria to determine the storage period, (2) the right to access, rectification, erasure, restriction, objection, and data portability, (3) the right to withdraw consent, (4) the right to lodge a complaint with a supervisory authority, (5) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract and whether the data subject is obliged to provide the personal data and the possible consequences of failure to provide that data, (6) the existence of automated decision-making, its significance, and consequences.[100]

Prior to further processing of personal data, the controller must also provide the data subject with information on the new purpose.[101]

Where personal data were obtained from the data subject, this information obligation must be fulfilled when the data is collected. In case personal data were not obtained from the data subject, this obligation must be fulfilled within one month from collection, or at the latest at the time of first communication or disclosure.[102]

Finally, in accordance with the principle of transparency, all this information must be provided in a concise, transparent, intelligible, and easily accessible form, while using clear and plain language.[103]

2.2.6.2 Right of access

According to Article 15 of the GDPR, the data subject has the right to obtain confirmation from the controller as to whether 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 specified under Article 15, which largely corresponds with the information to be provided under the right to information of Articles 13 and 14. The data subject may also request a copy of the data undergoing any processing.[104]

If the controller is able to demonstrate it is not in a position to identify the data subject, articles 15 to 20 (i.e. the data subject rights) will not apply, unless the data subject provides additional information enabling his/her identification.[105]

2.2.6.3 Right to rectification

In accordance with the principle of accuracy, the data subject has the right to the rectification of inaccurate personal data concerning him/her without undue delay. This also applies to incomplete

[99] Article 13 (1) and 14 (1) of the GDPR.
[100] Article 13 (2) and 14 (2) of the GDPR.
[101] Article 13 (3) and 14 (4) of the GDPR.
[102] Article 13 (1) and 14 (3) of the GDPR.
[103] Article 12 of the GDPR.
[104] Article 15 (3) of the GDPR: "*The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs.*"
[105] Article 11 (2) of the GDPR.

information, which should be completed by the controller, including by means of a supplementary statement.[106]

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

The data subject has the right for his/her personal data to be erased by the controller without undue delay provided one of the legitimate grounds for erasure is demonstrated.[107] This right cannot be exercised by the data subject where it is limited by one of the specified exceptions.[108] Furthermore, Article 17 (2) compels controllers that have made personal data public to inform other controllers which are processing personal data of the data subject for which erasure was requested. To achieve this, the controller should take reasonable steps, taking into account the available technology and cost of implementation.[109]

The exercise of this right is a difficult challenge from a technical perspective, since the architectures of some systems do not allow for complete erasure of personal data (e.g. blockchain technology).

2.2.6.5 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. This is the case when: (1) the data subject disputes data accuracy, (2) the processing is unlawful but the data subject objects to erasure and requests restriction instead, (3) the controller has no further need for the data but the data subject requires the personal data to establish, exercise, or defend legal claims, and (4) when the data subject objects to the processing pursuant to Article 21 (1).[110]

The restriction of data processing means the controller may store the personal data, but any further processing can only take place: (1) with the data subject's consent, (2) for the establishment, exercise or defense of legal claims, (3) for the protection of the rights of another natural or legal person, or (4) for reasons of important public interest of the Union or of a Member State.[111]

2.2.6.6 Right to data portability

While the right to 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 even entitled to demand that personal data is transmitted directly from one controller to another.[112]

However, portability is narrower in scope than the right to data access, as it only applies to personal data which is processed by automated means (e.g. no paper records), which the data subject has

[106] Article 16 of the GDPR.

[107] Grounds for erasure in Article 17 (1) of the GDPR: (a) the personal data are no longer necessary in relation to the purpose for which they were collected or otherwise processed, (b) the data subject withdraws consent and there is no other legal ground for the processing, (c) the data subject objects to the processing and there is no overriding legitimate grounds for processing, (d) the personal data have been unlawfully processed, (e) for compliance with legal obligation, (e) the personal data have been collected in relation to the offer of information society services.

[108] Exceptions for erasure in Article 17 (3) of the GDPR : (a) the right of freedom of expression and information, (b) compliance with a legal obligation, a task in the public interest or in the exercise of official authority, (c) reasons of public interest in the area of public health, (d) proportional archiving, research, or statistical purposes, (e) and for the establishment, exercise or defence of legal claims.

[109] Article 17 (2) of the GDPR.

[110] Article 18 (1) of the GDPR.

[111] Article 18 (2) of the GDPR.

[112] Article 20 (1) and (2) of the GDPR.

provided to the controller, and only where the legal basis for processing is consent or fulfilment of a contract.[113]

2.2.6.7 Right to object

Every data subject has the right to object three types of processing, namely: 1) the processing based on a legitimate interest[114] or because it's necessary for a task in the public interest or in the exercise of official authority[115], (2) the processing for direct marketing purposes, and 3) the processing for scientific, historical, research or statistical purposes. In case of the first type of processing, the controller must cease processing activities unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.[116] For the second type of processing, the controller must simply cease processing. In case of the third type of processing, the controller must cease processing activities unless the processing is necessary for the performance of a task carried out for reasons of public interest.[117]

2.2.6.8 Restrictions to data subject 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. 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.[118]

[113] Article 20 (1) of the GDPR.
[114] Article 6 (1) (f) of the GDPR.
[115] Article 6 (1) (e) of the GDPR.
[116] Article 21 (1) of the GDPR.
[117] Article 21 (6) of the GDPR.
[118] Article 23 (1) of the GDPR.

3 Electronic identification and trust services framework

3.1 The Regulation on electronic identification and trust services for electronic transactions

The eIDAS Regulation[119] entered into force on the 17th of September 2014 and is applicable since the 1st of July 2016. The Regulation aims to ensure that individuals and businesses can securely utilize their own national electronic identification schemes (eIDs) to access services in other EU countries where eIDs are available and to create a European internal market for electronic trust services. It lays down conditions for mutual recognition of eIDs by other Member States, as well as rules for trust services. Furthermore, the eIDAS regulation establishes a legal framework for electronic signatures, electronic seals, electronic time stamps, electronic documents, electronic registered delivery services, and qualified certificates for website authentication.[120]

The implementation of a Self-Sovereign Identity (SSI) management system in KRAKEN aims to give the users full control over their digital identity without relying on a centralized entity. The eIDAS framework, applicable to electronic identification and trust services, is therefore crucial for the success of the KRAKEN project. For this reason, the current chapter aims to give an overview of the most important concepts and principles found in the eIDAS framework.

Chapter II of the eIDAS Regulation lays down rules on electronic identification (e.g. mutual recognition, notification, and cross-border use) and Chapter III on trust services (e.g. qualified trust services, electronic signatures, electronic seals, electronic timestamps, etc.)

3.1.1 Scope of application

The eIDAS Regulation applies to eIDs that have been notified by a Member State and to trust service providers (TSP's) that are established in the Union. It does not apply to the provision of trust services that are used exclusively within closed systems resulting from national law or from agreements between a defined set of participants.[121]

The Regulation also makes clear that the processing of personal data must be carried out in accordance with the GDPR and the principles contained therein.[122] Recital 11 of the Regulation explicitly states that authentication for an online service should concern processing of only those identification data that are adequate, relevant and not excessive to grant access to that service online. It also stresses that trust service providers and supervisory bodies should respect the principle of confidentiality and security of processing, as required by the GDPR. Finally, Article 12 requires that the notified electronic identification schemes shall be interoperable. For this reason, an interoperability framework shall be established that meets, among others, the following criteria:

> *"(c) it facilitates the implementation of the principle of privacy by design; and*
>
> *(d) it ensures that personal data is processed in accordance with Directive 95/46/EC[123]."[124]*

[119] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (eIDAS Regulation).

[120] Article 1 of the eIDAS Regulation.

[121] Article 2 (1) and (2) of the eIDAS Regulation.

[122] Article 5, 12, and Recital 11 of the eIDAS Regulation.

[123] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data; repealed and replaced by the GDPR.

[124] Article 12 of the eIDAS Regulation.

The Regulation does not further elaborate on the requirement of privacy by design, although a similar concept can be found in Article 25 of the GDPR[125], which also has to be respected according to Article 5, 12, and Recital 11 of the eIDAS Regulation.

3.1.2 Electronic identification

3.1.2.1 Mutual recognition and notification

The eIDAS Regulation creates the obligation for a Member State to recognize electronic identification means[126] of other Member States when electronic identification[127] is required to access an online service provided by a public sector body in the first Member State.[128] As a condition, the electronic identification means to be recognized must be included as an electronic identification scheme[129] in a list published by the European Commission.[130] This list contains electronic identification schemes that have been notified by the Member States and have been subsequently accepted. A notification to the European Commission must contain basic information, such as; a description of the scheme, its assurance levels, the issuers, the supervisory regime, information on the liability regime, etc.[131] In order to be eligible for notification to the European Commission, the electronic identification scheme must first satisfy a number of conditions, including that; it can be used to access at least one service by a public sector body which requires electronic identification, it meets the requirements of at least one of the Levels of Assurance (LoAs), it meets the requirements set out in the implementing act, etc.[132]

3.1.2.2 Levels of Assurance

The eIDAS Regulation establishes LoAs as a way to indicate the degree of confidence in a system.[133] Recital 16 of the Regulation describes LoAs as a way to "*characterize the degree of confidence in electronic identification means in establishing the identity of a person, thus providing assurance that the person claiming a particular identity is in fact the person to which that identity was assigned."* Article 8 of the Regulation goes on to define three levels of LoAs; (1) low, (2) substantial, and (3) high:

> (1) LoA 'low' refers to an electronic identification means which provides a limited degree of confidence in the claimed identity of a person. It is further characterized by technical specifications, standards, and procedures aimed at decreasing the risk of misuse or alteration of the identity.[134]
>
> (2) LoA 'substantial' refers to an electronic identification means which provides a substantial degree of confidence in the claimed identity of a person. It is further characterized by technical

[125] Data protection by design and by default.

[126] Article 3 (2) of the eIDAS Regulation defines 'electronic identification means' as "*a material and /or immaterial unit containing person identification data and which is used for authentication for an online service;".* Article 3 (3) defines 'person identification data' as "*a set of data enabling the identity of a natural or legal person, or a natural person representing a legal person to be established;".*

[127] Article 3 (1) of the eIDAS Regulation defines 'electronic identification' as "*the process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person;".*

[128] Article 6 (1) of the eIDAS Regulation.

[129] Article 3 (4) of the eIDAS Regulation defines 'electronic identification scheme' as *"a system for electronic identification under which electronic identification means are issued to natural or legal persons, or natural persons representing legal persons;".*

[130] Article 6 (1) (a) of the eIDAS Regulation.

[131] Article 9 (1) of the eIDAS Regulation.

[132] Article 7 of the eIDAS Regulation.

[133] Article 8 of the eIDAS Regulation.

[134] Article 8 (2) (a) of the eIDAS Regulation.

> specifications, standards, and procedures aimed at substantially decreasing the risk of misuse or alteration of identity.[135]
>
> (3) LoA 'high' refers to an electronic identification means which provides a higher degree of confidence in the claimed identity of a person. It is further characterized by technical specifications, standards, and procedures aimed at preventing misuse or alteration of identity.[136]

3.1.3 Trust services

As mentioned before, the eIDAS Regulation establishes a legal framework for trust services, specifically electronic signatures, electronic seals, electronic time stamps, electronic documents, electronic registered delivery services, and qualified certificates for website authentication. This section will focus on electronic signatures and their requirements.

The eIDAS Regulation defines a ***trust service*** as:

> *"an electronic service normally provided for remuneration which consists of:*
>
> *(a) the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or*
>
> *(b) the creation, verification and validation of certificates for website authentication; or*
>
> *(c) the preservation of electronic signatures, seals or certificates related to those services;"*[137]

A distinction is made between normal trust services and ***qualified trust services***. To gain the status of a qualified trust service, it is necessary that the trust service satisfies a number of requirements, which may vary between specific trust services.

The entities that provide one or more (qualified) trust services are called ***(qualified) trust service providers.***[138] The Regulation imposes certain obligations on TSP's, such as the obligation to take appropriate technical and organizational measures to manage the risks posed to the security of their trust services. This risk-based approach obliges TSP's to prevent and minimize the impact of security incidents and notify the relevant authorities of any breach of security or loss of integrity of its services.[139]

3.1.3.1 Electronic signatures

The eIDAS Regulation defines the three types of electronic signatures as follows:

> *"'**electronic signature'** data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign;".*
>
> *"'**advanced electronic signature'** means an electronic signature which meets the requirements set out in Article 26;".*
>
> *"'**qualified electronic signature'** means an advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures;".*[140]

An advanced electronic signature must satisfy four cumulative requirements; (1) it is uniquely linked to the signatory, (2) it is capable of identifying the signatory, (3) it is created using electronic signature

[135] Article 8 (2) (b) of the eIDAS Regulation.

[136] Article 8 (2) (c) of the eIDAS Regulation.

[137] Article 3 (16) of the eIDAS Regulation.

[138] Article 3 (19) and (20) of the eIDAS Regulation

[139] Article 19 (1) and (2) of the eIDAS Regulation.

[140] Article 3 (10), (11), and (12) of the eIDAS Regulation.

creation data that the signatory can, with a high level of confidence, use under his sole control, and (4) it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable.[141] In its implementing Decision (EU) 2015/1506, the Commission laid down specifications for formats of advanced electronic signature to be recognized by public sector bodies. If an electronic signature satisfies these specifications, there exists an assumption that the electronic signature fulfils the requirements of an advanced electronic signature.[142]

A qualified electronic signature, on the other hand, satisfies all the requirements of an advanced electronic signature, in addition to two more requirements; (1) it is created by a qualified electronic signature creation device, and (2) it is based on a qualified certificate for electronic signatures. The eIDAS Regulation also includes a list of requirements that a qualified electronic signature creation device and a qualified certificate for electronic signatures must satisfy.[143]

Furthermore, the Regulation establishes that an electronic signature shall not be denied legal effect or admissibility in legal proceedings solely on the grounds that it is in an electronic form. It is also not necessary for an electronic signature to meet the requirements of a qualified electronic signature in order to be considered valid.[144] However, it is still advantageous to use a qualified electronic signature, since it has the equivalent legal effect of a handwritten signature.[145]

The eIDAS Regulation also has its implication for technologies that make use of blockchain. Looking at the definition of ***electronic documents***, it is clear that the data contained in blockchains would qualify as such, since this data is in fact “*any content stored in electronic form, in particular text or sound, visual or audiovisual recording;”.*[146] Consequently, this data cannot be denied legal effect solely on the grounds that it is in electronic form.[147] With regard to electronic signatures, it is not yet fully clear whether a transaction on a blockchain can be considered to be signed and which level of electronic signature it would have.[148]

[141] Article 26 of the eIDAS Regulation.
[142] Article 27 (5) of the eIDAS Regulation; and Commission Implementing Decision (EU) 2015/1506 of 8 September 2015 laying down specifications relating to formats of advanced electronic signatures and advanced seals to be recognised by public sector bodies pursuant to Articles 27(5) and 37(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market.
[143] Annex II and I of the eIDAS Regulation.
[144] Article 25 (1) of the eIDAS Regulation.
[145] Article 25 (2) of the eIDAS Regulation.
[146] Article 3 (35) of the eIDAS Regulation.
[147] Article 46 of the eIDAS Regulation.
[148] The European Union Blockchain Observatory and Forum, Thematic Report on Blockchain and Digital Idenitity, 2019, 21.

4 Privacy metrics

This chapter provides some general information on the concept of privacy metrics; what they are, their objectives, and the different types that could be relevant for the KRAKEN project. Privacy metrics provide users with valuable information on the protection of their privacy in a system and contribute to the transparency of processing while giving more control to the users. The chapter concludes by identifying several considerations and parameters for the selection of privacy metrics in KRAKEN.

4.1 Objectives

Privacy is a fundamental human right. It can be defined as "*the ability of an individual to control the terms under which personal information is acquired and used.*"[149]. It represents an active attribute giving the user control over his/her personal data. In the context of information processing, privacy focusses more on contextual integrity, which means that it is decisive in which context the personal information is collected and used.[150]

The measures protecting the personal information can be policies, regulations and – with mandatory technical controls – **privacy enhancing technologies (PETs)**. PETs protect privacy based on technology rather than policy and can thus offer much stronger protection; they can be analyzed formally by system theory and can be measured and compared to each other.[151]

Accordingly, a **privacy metric** is defined as a "*degree of privacy enjoyed by users in a system and the amount of protection offered by privacy-enhancing technologies*"[152]. More actively worded, privacy metrics are "*measures to determine the susceptibility of data or a dataset to revealing private information*"[153]. These measures include the combination of private data, level of detail, correctness of information and possible background information, including personal data. Thus, the privacy metrics are a key element to give control to data subjects. For KRAKEN, it is necessary to explicitly control the access by specific data subjects.

Summarizing, the **objectives** of privacy metrics are[154]:

- to measure the degree of privacy enjoyed by users in a system
- the amount of protection offered by privacy-enhancing technologies
- to contribute to the improvement of user privacy in the digital world
- for determining the susceptibility of data or a dataset to revealing private information
- the ability to link private data to an individual, the level of detail or correctness of sensitive information

[149] A. F. WESTIN, "Privacy and freedom", *New York: Atheneum*, 1967, Vol. 7, 431 – 453.

[150] H. NISSENBAUM, "Privacy as contextual integrity," *Wash. L. Rev.*, 2004, Vol. 79, 119.

[151] I. WAGNER and D. ECKHOFF, "Technical privacy metrics: a systematic survey," *ACM Computing Surveys (CSUR)*, 2018, Vol. 51, No. 3, 1–38.

[152] Ibid.

[153] C. CLIFTON, "Privacy Metrics" In: L. LIU and M.T. ÖZSU (eds) *Encyclopedia of Database Systems*, *Springer,* Boston, MA, 2009, 2137–2139, available at http://link.springer.com/10.1007/978-0-387-39940-9_272 (last accessed on 21 July 2020).

[154] I. WAGNER and D. ECKHOFF, "Technical privacy metrics: a systematic survey," *ACM Computing Surveys (CSUR)*, 2018, Vol. 51, No. 3, 1–38.

There are a wide number of privacy metrics available[155], many of which were developed over the last years for multiple purposes. It is therefore crucial to select the optimal form of a privacy metric for a specific scenario. Beside the planned application domain and the foreseen focus points, it is necessary to analyze appropriate criteria for categorization based on the application requirements. In the KRAKEN project, some specific **requirements** for the application of privacy metrics have been stated:

- easy to understand for non-experts
- good usability, individually configurable
- providing security, privacy, transparency
- usable interface for end-users, data subjects
- presented in an understandable way
- focus on a data market platform, control of private data by the owner (end-user) to gather, store, transport, update, correct, analyze, share, and monetize the personal data.

The user decides how much privacy should be revealed based on the applied privacy metrics. However, mediated data are not stored.

4.2 Fundamentals

Due to the wide range of available privacy metrics, we suggest a **fundamental approach** for establishing a privacy metric:

Step 1: A structured risk analysis allows users to understand the precise privacy risk, enriched with advice from an external advisory board, policy makers, and/or consumer protection authorities.

Step 2: The privacy metric takes properties of a system as an input, amount of sensitive information leaked, and the number of users who are indistinguishable with respect to some characteristic.

Step 3: This step yields a numerical (or canonical) value to quantify the privacy level in a system.

Step 4: The different PETs are compared. In order to judge the efficiency of PETs, privacy metrics are needed that can measure the level of privacy in a system, or the privacy provided by a given PET.

As a prerequisite for conducting a detailed and systematic risk analysis in Step 1, the KRAKEN use cases need to be specified in advance. Currently, four use cases are being discussed:

- data sharing of LinkedIn certificates
- fitness tracker as medical application
- educational use case in a university context
- data sharing for defined applications with threat of invasion of privacy

In order to select a privacy metric, one is faced with one or more of the following **challenges**. Firstly, one must cope with the diversity and complexity of privacy metrics in the literature. So far, no structured and comprehensive overview exists and new metrics are proposed frequently due to their application in different domains. Additionally, privacy studies are often incomparable and it is difficult to select an optimal metric for the upcoming requirements of the focused applications in specific circumstances. Hence, it is necessary to follow a transparent and efficient selection process based on defined selection criteria when identifying the optimal privacy metric. Wagner and Eckhoff[156] suggest

[155] Ibid.
[156] Ibid.

nine decision questions to address this challenge in an efficient way. We will be mainly following this approach for selecting the appropriate privacy metric in KRAKEN, as described in section 4.3.

Secondly, there still exist interfering effects. For instance, actions of one user can affect the privacy of other users (i.e. an interdependency of privacy). A sufficiently large set of people or a sufficiently large part of the population is required to ensure privacy. Furthermore, the aggregation of metrics can lead to biased results and complicates its visualization. Additionally, a combination of metrics considers values of different privacy metrics for one entity, which counteracts the comparison capability. It should rather be avoided to establish a new privacy metric to overcome this problem [2, p. 37f].

Thirdly, there is a challenge ensuring sufficient quality and how it should be measured. In addition, metrics can also measure users' privacy attitudes, behaviors, or perceptions. However, in this work we only focus on technical privacy metrics.

Despite the wide range of available privacy metrics, they share common characteristics and can be classified according to three different categories:

- the adversary model
- the data sources and inputs for computation of metrics and
- the output measures

Adversary Model

The adversary intends to compromise users´ privacy (e.g. by de-anonymization of datasets) and learns sensitive information and/or users' properties. Obviously, more powerful adversaries (i.e. those with more resources or prior knowledge) can target users' privacy more effectively. In the literature, we find a taxonomy of adversary types and their capabilities in Diaz et. Al.[157].

In the context of adversary-related privacy metrics, the following characteristics of adversaries can be distinguished:

- *Local vs. global*: global adversaries have access to the entire system, whereas local adversaries can only access parts of the system.
- *Active vs. passive*: passive adversaries can only read or observe the system, whereas active ones can interfere and add, remove or modify information and use that to their advantage.
- *Internal vs. external*: external adversaries are not part of the system, whereas internal adversaries are acting from within the system, e.g. because they are working for service providers or third parties controlling specific components of the system.
- *Static vs adaptive*: adaptive adversaries can change their attack strategy (e.g. by learning systems parameters through observations) and react to counter measures, which makes them more powerful. Static adversaries stick to their attack strategy irrespective of the progress of their attack.
- *Prior knowledge*: some adversaries may have general domain-specific or scenario-specific knowledge, which can strengthen their attack capabilities considerably.
- *Resources*: with regards to given computational resources, efficient adversaries are restricted to probabilistic polynomial-time algorithms, whereas unbounded adversaries are not restricted to any computational model. Such an unbounded adversary model is often used to evaluate the privacy by considering future technological advancements.

[157] C. Díaz, S. Seys, J. Claessens and B. Preneel, "Towards Measuring Anonymity" In: R. Dingledine and P. Syverson (eds) Privacy Enhancing Technologies (PET 2002), Lecture Notes in Computer Science, *Springer*, Berlin, 2003, Vol. 2482, 54-68.

Input and Data Sources

Data sources and the availability of input data determine whether a metric can be used in a specific context or scenario. Each privacy metric has a specific set of input parameters required to perform the computation; if one of the parameters is not available, the privacy metric might not be applicable to the respective scenario (or provide false or insufficient results). To summarize the required parameters, the following high-level categories can be used (cf. also Wagner and Eckhoff[158]):

- *Adversary´s estimate*: the adversary´s estimate is the result to breach privacy computed by the adversary. It is usually described in mathematical terms, often in the form of a probability distribution.
- *Adversary´s resources*: the adversary´s resources can be described in terms of bandwidth, computational power, time, etc.
- *True outcome*: the true outcome is the ground truth. It is obviously not available to the adversary but is used to describe sensitive data and to judge how good the adversary´s estimate is.
- *Prior knowledge*: prior knowledge describes the scenario-specific knowledge of the adversary. Like the adversary's estimate, it is usually modelled as a prior probability distribution.
- *Parameters*: various parameters can be relevant to configure a specific privacy metric, for example an order to describe the sensitivity of parameters or threshold values to describe the desired privacy levels.

Output Measures

The output of a privacy metric is directly related to the kind of property that the metric measures. It is therefore important in this context to keep the requirements of the given scenario in mind, where the privacy metric will be used, and which goals should be achieved by using the metric. The relevant categories are the following (according to Wagner and Eckhoff[159]):

- *Uncertainty*: uncertainty metrics are based on the assumption that the privacy of a system is high if the uncertainty of the adversary´s estimates is high.
- *Information gain or loss*: in relation to information theory, the amount of privacy lost based on the disclosure of information or the amount of information gained by the adversary is measured by privacy metrics focusing on information gain or loss.
- *Data similarity*: data similarity metrics measure the similarity of data either within a dataset or between two sets of data. In this way, these metrics abstract from the adversary and focus on properties of data.
- *Indistinguishability*: metrics based on indistinguishability analyze the various outcomes of the privacy mechanisms. If the adversary cannot distinguish between any pairs of outcomes, the privacy is considered high.
- *Adversary´s success probability*: metrics using the success probability describe the likelihood of the adversary´s attempt to reveal privacy. In this way, low success probability correlates with high levels of privacy.
- *Error*: error-based metrics measure the correctness of the adversary´s estimate (i.e. the distance between the correct outcome and the prior estimate). In this context, high correctness directly relates to a low privacy level.

[158] I. WAGNER and D. ECKHOFF, "Technical privacy metrics: a systematic survey," *ACM Computing Surveys (CSUR)*, 2018, Vol. 51, No. 3, 1–38.
[159] Ibid.

- *Time*: time-based metrics consider the time until the adversary succeeds in breaking the privacy of the system. Longer times correlate to higher privacy levels.
- *Accuracy or precision*: some privacy metrics quantify how precise the adversary´s estimates are. More precise estimates correspond to a lower privacy.

4.3 Selecting privacy metrics for KRAKEN

Privacy metrics cannot directly measure users' privacy. Rather, they measure quantities which are related to privacy and, as described in section 4.1 and 4.2, there exists a huge number of different metrics.

Choosing the adequate privacy metrics for KRAKEN will therefore strongly depend on the final definition of the use cases in the project (as already pointed out in section 4.2). After WP2 has defined the system components and the architecture as well as a detailed description of the different use cases, the specific privacy metric types can be selected. In the selection process for the privacy metrics of KRAKEN, we will again follow the recommendations of Wagner and Eckhoff[160]. They propose to consider at least seven different dimensions when choosing privacy metrics:

1. The main criterion is how the privacy of the use cases can be described and quantified. Is it required to give privacy guarantees or is it more appropriate to quantify privacy levels? Regarding the quantification of privacy levels, the average and worst case as well as the distribution of privacy are considered.
2. The characteristics of the adversary are also important (as already mentioned in section 4.2). However, many papers on new PETs use accuracy, similarity, and indistinguishability metrics and are thus rather abstract from the adversary's capabilities (as they are often not entirely known).
3. The third question that needs to be evaluated for each use case is the respective data that needs to be protected.
4. The availability of input data for each use case is an important parameter when choosing a privacy metric (as already mentioned in section 4.2). Obviously, we can discard all privacy metrics from the literature for which the necessary input data are not available in the respective use case scenarios.
5. Since we mainly expect experts to read the final report of KRAKEN, we will not restrict our privacy metrics selection by the question of target audience.
6. After describing the use cases in detail, we will start a small literature research to investigate whether there are publications on privacy metrics on similar applications. If we find relevant publications, the same privacy metrics might be applicable for the KRAKEN use cases. This will also allow for easier comparison between our results and the published studies.
7. With respect to the implementation of the metrics, we will follow a pragmatic strategy and only choose such metrics which already have been implemented in different application areas.

After the discussion and selection process, the optimal privacy metrics for each use case can be implemented.

[160] Ibid.

5 Conclusion

This deliverable provides a preliminary high-level overview and analysis of the legal frameworks applicable to KRAKEN. These legal frameworks (i.e. the privacy/data protection and electronic identification frameworks) contain numerous important concepts and principles which need to be taken into account in the course of the project and development of KRAKEN technologies.

As the main piece of legislation in the EU data protection regime, the GDPR plays an important role in KRAKEN. It lays down a number of essential data protection principles which have to be respected at all times; before, during, and after processing. One of these data protection principles states that processing must be lawful; meaning that the processing activities must be legitimate and rely on a valid legal basis. In KRAKEN, consent will be the most important legal basis. Although the most well-known legal basis, obtaining valid consent can be difficult considering the strict requirements for validity. According to the principle of accountability, the controller must also be able to provide evidence of consent, which can be achieved in various ways, for example through a dynamic consent application. Taking into account the risk-based approach of the GDPR, it is also important to always assess the potential risks of processing to the data subject and implement appropriate technical and organizational measures to prevent or minimize these risks. When processing sensitive personal data, such as medical or health data, additional attention should be given to these potential risks. The data subject must also be able to exercise its rights vis-à-vis the controller, which should be easily accessible. The application of the GDPR also brings with it a number of questions. Applying concepts such as 'identifiability', 'anonymization', 'controller', and 'processor' requires a factual assessment of the circumstances. In the context of a research project, these circumstances may not always be apparent or may be subject to change.

Although not analyzed in this deliverable, the possibility to monetize and transact personal data is a crucial element for the success of the KRAKEN project. The monetization of personal data is not explicitly prohibited under the international and EU data protection regime, as long as the applicable legislation (i.e. the GDPR) is complied with. The possibility to process personal data in such a way will therefore depend on national legislation, specifically national implementations of the GDPR and national contract law. This topic will be further explored in D7.2, which will also provide an overview of national rules covering the monetization of personal data.

Secondly, the eIDAS Regulation is an important piece of legislation for systems involving electronic identification. It also lays down specific rules and requirements for electronic signatures and certificates, including with regard to their legal effects.

Finally, the introduction of privacy metrics in a system contributes to the overall level of privacy enjoyed by the users. There are many different types of privacy metrics, each with their own objectives and requirements. Consequently, it is important to identify relevant considerations and parameters for the selection of appropriate privacy metrics in KRAKEN. The actual selection of privacy metrics is dependent on the specification of the system architecture and use cases. For this reason, the selection process will be further explored in future deliverables.

The current deliverable, D2.1, will feed into D7.2, which falls under T7.2. This task builds on the identified ethical and legal frameworks in order to provide a set of specific ethical and legal requirements and implementation guidelines. Furthermore, a deeper analysis of ethical and legal issues related to broader aspects of KRAKEN will be conducted. This task will be additionally fed by input from technical partners, where necessary.

6 Bibliography

Legislation

Primary sources

Charter of Fundamental Rights of the European Union, OJ C 202/2, 7.6.2016, p. 389-405.

Council of Europe, Convention for the Protection of Human Rights and Fundamental Freedoms, 4 November 1950.

Secondary sources

Commission Implementing Decision (EU) 2015/1506 of 8 September 2015 laying down specifications relating to formats of advanced electronic signatures and advanced seals to be recognised by public sector bodies pursuant to Articles 27(5) and 37(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market.

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

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.

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.

Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

Jurisprudence

European Court of Human Rights

European Court of Human Rights, *Airey v. Ireland*, Judgement of 9 October 1979, no. 6289/73.

European Court of Human Rights, *Costello-Roberts v. the United Kingdom,* Judgement of 25 March 1993, no. 13134/87.

European Court of Human Rights, *Dudgeon v. The United Kingdom*, Judgement of 22 October 1981, no. 7525/76.

European Court of Human Rights, *Leander v. Sweden*, Judgement of 26 March 1987, no. 9248/81.

European Court of Human Rights, *S and Marper v. the United Kingdom*, Judgement of 25 August 1997, no. 20837/92.

European Court of Human Rights, *Silver and Others v. the United Kingdom,* Judgement of 25 March 1983.

European Court of Human Rights, *Von Hannover v. Germany (no. 2)*, Judgement of 7 February 2012.

European Court of Human Rights*, Z. and Others v. the United Kingdom*, Judgement of 10 May 2001, no.29392/95.

European Court of Human Rights, *Z v. Finland*, Judgement of 25 February 1997, no. 22009/93.

Court of Justice of the European Union

Court of Justice of the European Union, *Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV,* Judgement of 29 July 2019, C-40/17.

Court of Justice of the European Union, *Patrick Breyer v. Bundesrepublik Deutschland*, Judgement of 19 October 2016, C-582/14.

Court of Justice of the European Union, *Stauder*, Judgement of 12 November 1969, C-29/69.

Court of Justice of the European Union, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH,* Judgement of 5 June 2018, C-210/16.

Doctrine

Books and articles

CLIFFORD, D. and AUSLOOS, J., Data Protection and the Role of Fairness, KU Leuven Centre for IT & IP Law, CiTiP Working Paper 29/2017, 3 August 2017, 44 p.

CLIFTON, C., "Privacy Metrics" In: LIU, L. and ÖZSU, M.T. (eds) *Encyclopedia of Database Systems*, *Springer,* Boston, MA, 2009, 2137–2139, available at http://link.springer.com/10.1007/978-0-387-39940-9_272 (last accessed on 21 July 2020).

DÍAZ, C., SEYS, S., CLAESSENS, J. and PRENEEL, B., "Towards Measuring Anonymity" In: DINGLEDINE, R. and SYVERSON, P. (eds) Privacy Enhancing Technologies (PET 2002), Lecture Notes in Computer Science, *Springer*, Berlin, 2003, Vol. 2482, 54-68.

NISSENBAUM, H., “Privacy as contextual integrity,” *Wash. L. Rev.*, 2004, Vol. 79, 119.

The European Union Agency for Fundamental Rights, the Council of Europe, and the European Data Protection Supervisor, Handbook on European data protection law, 2018, 397 p.

The European Union Blockchain Observatory and Forum, Thematic Report on Blockchain and Digital Idenitity, 2019, 27 p.

The European Union Blockchain Observatory and Forum, Thematic Report on Blockchain and the GDPR, 2018, 36 p.

WAGNER, I. and ECKHOFF, D., “Technical privacy metrics: a systematic survey,” *ACM Computing Surveys (CSUR)*, 2018, Vol. 51, No. 3, 1–38.

WESTIN, A.F., “Privacy and freedom", *New York: Atheneum*, 1967, Vol. 7, 431 – 453.

Article 29 Data Protection Working Party

Article 29 Data Protection Working Party, Guidelines on consent under Regulation 2016/679, 28 November 2017 and last revised and adopted on 10 April 2018, 17/EN, WP259 rev.01, 31 p.

Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, 2 April 2013, 00569/13/EN, WP203, 70 p.

Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymization Techniques, 10 April 2014, 0829/14/EN WP216, 37 p.

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, 68 p.

European Data Protection Board

European Data Protection Board, Guidelines 05/2020 on consent Under Regulation 2016/679, 4 May 2020, 33 p.

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, 9 April 2019, 16 p.

European Data Protection Supervisor

European Data Protection Supervisor, A preliminary Opinion on data protection and scientific research, 6 January 2020, 35 p.

European Data Protection Supervisor, Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725, 7 November 2019, 34 p.

KRAKEN

www.krakenh2020.eu

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 871473