BROKERAGE AND MARKET PLATFORM FOR PERSONAL DATA

D7.3 Ethical and legal evaluation and recommendations

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

D7.3 Ethical and legal evaluation and recommendations

Grant agreement	871473
Work Package Leader	KU Leuven
Author(s)	Wim Vandevelde (KU Leuven), Jessica Schroers (KU Leuven)
Contributors	Anton Vedder (KU Leuven)
Reviewer(s)	Silvia Gabrielli (FBK), Karl Koch (TUG), Christof Rabensteiner (TUG)
Version	Final
Due Date	30/11/2022
Submission Date	29/11/2022
Dissemination Level	Public

Copyright

© KRAKEN consortium. This document cannot be copied or reproduced, in whole or in part for any purpose without express attribution to the KRAKEN project.

Release History

Version	Date	Description	Released by
v0.1	20/07/2022	Draft table of contents	Jessica Schroers (KUL), Wim Vandevelde (KUL)
v0.2	07/11/2022	Final draft version for review	Jessica Schroers (KUL), Wim Vandevelde (KUL)
v0.3	28/11/2022	Final version after review	Jessica Schroers (KUL), Wim Vandevelde (KUL)
v1.0	29/11/2022	Submitted version	Atos

Table of Contents

1 Introduction 10

1.1 Purpose of the document 10

1.2 Structure of the document 10

2 Upcoming legislation 11

2.1 The Data Governance Act 11

2.1.1 What is it and what does it aim for? 11

2.1.2 Would KRAKEN be a data intermediation service provider? 11

2.1.3 Are Data Unions providing ‘services of data cooperatives’? 12

2.1.4 Could KRAKEN be a data altruism organization? 12

2.1.5 Requirements for KRAKEN as data intermediation service provider 13

2.1.6 Requirements for Data cooperatives 14

2.1.7 Requirements if KRAKEN would be a data altruism organization 14

2.1.8 How does the notification/registration procedure work? 16

2.1.9 Who is the competent authority? 17

2.1.10 What if a DISP does not comply with the DGA requirements? 17

2.1.11 European data altruism consent form 18

2.2 The Data Act Proposal 18

2.2.1 What is it and what does it aim for? 18

2.2.2 What is important for KRAKEN? 18

2.3 The Digital Identity Regulation Proposal 19

2.3.1 What is it and what does it aim for? 19

2.3.2 What is important for KRAKEN? 20

2.4 The European Health Data Space Proposal 22

2.4.1 What is it and what does it aim for? 22

2.4.2 What is important for KRAKEN? 22

2.5 The Digital Services Act 23

2.5.1 What is it and what does it aim for? 23

2.5.2 Scope of application 23

2.5.3 Layered obligations 24

2.5.4 What is important for KRAKEN? 28

2.6 The Data Markets Act 29

2.6.1 What is it and what does it aim for? 29

2.6.2 Scope of application 30

2.6.3 Obligations for gatekeepers 31

2.6.4 What is important for KRAKEN? 31

3 Ethical and legal evaluation of KRAKEN 32
3.1 Analysis KRAKEN as a controller for account data 32
3.2 Analysis KRAKEN as a data exchange service 37
3.3 Analysis KRAKEN as an analytics provider 41
3.4 Analysis KRAKEN as a provider of an information society service 43
3.5 Update on legal and ethical aspects of the pilots 46
3.5.1 First pilot in October and November 2021 46
3.5.2 Final pilot in September 2022 47
3.6 Recommendations 48
4 Lightweight development Data Protection Impact Assessment 49
5 Self-sovereign identity 51
6 Open issues and recommendations for policy-makers 53
6.1 The role and implications of blockchain in KRAKEN 53
6.2 Roles and responsibilities under the GDPR 54
6.3 The anonymization of personal data 56
6.4 Consent as a legal basis 58
6.5 The monetization of personal data 60
7 Conclusion 62
8 Bibliography 64
Annexes 67
Requirements for KRAKEN as a controller of account data 67
Requirements for KRAKEN as a data exchange service provider 75
Requirements for KRAKEN as data analytics provider 85
Requirements for KRAKEN as a provider of an information society service 93
DPIA table account data 95
DPIA table batch data 104
DPIA table data analytics 114

List of Tables

Table 1. Requirements for KRAKEN as a controller of account data ... 74
Table 2: Requirements for KRAKEN as data exchange service provider ... 84
Table 3: Requirements for KRAKEN as data analytics provider ... 92
Table 4: Requirements for KRAKEN as a provider of an information society service ... 94
Table 5: DPIA table account data ... 103
Table 6: DPIA table batch data ... 113
Table 8: DPIA table data analytics ... 121

List of Acronyms

Acronym	Description
AEPD	The Spanish Data Protection Authority
CJEU/ECJ	European Court of Justice
CNIL	Commission Nationale de l’Informatique et des Libertés
DA	Data Act
DGA	Data Governance Act
DID	Decentralized identifier
DISP	Data intermediation service provider
DMA	Digital Markets Act
DPA	Data Protection Authority
DPIA	Data Protection Impact Assessment
DPO	Data protection officer
DSA	Digital Services Act
EBSI	European Blockchain Services Infrastructure
EDIW	European Digital Identity Wallet
EDP	European Data Protection Board
EDPS	European Data Protection Supervisor
EEA	European Economic Area
eIDAS 2.0	Digital Identity Regulation
ESSIF	European self-sovereign identity framework
EU	European Union
FBK	Bruno Kessler Foundation
GDPR	General Data Protection Regulation
GUI	Graphical user interface
LIM	Legal Identity Manager
KRER	KRAKEN Revocation & Endorsement Registry
KTIR	KRAKEN Trusted Issuer Registry
KTSR	KRAKEN Trusted Schema Registry
KWCT	KRAKEN Web Company Tool
SMEs	Small and medium-sized enterprises
SMPC	Secure multi-party computation
SSI	Self-sovereign identity
TUG	Graz University of Technology
UI	User interface
VC	Verifiable Credential
VLOP	Very large online platform

Executive Summary

This deliverable is part of Work Package 7 – 'Ethical and Legal compliance', which aims to provide KRAKEN consortium members with the necessary guidance for the implementation of the applicable ethical and legal requirements. More specifically, it falls under Task 7.2 – 'Ethical and Legal Analysis and Evaluation', which assesses whether or not the ethical and legal requirements provided throughout the project have been taken into account. This includes an evaluation and validation of the ethical and legal requirements as well as recommendations to fill in the remaining gaps in implementation. Lastly, this deliverable formulates further policy recommendations based on the identified gaps and lessons learned.

There are several pieces of upcoming legislation that are of relevance for the KRAKEN project, even after the project has ended. Firstly, the Data Governance Act (DGA) has been adopted and will apply from 24 September 2023. This act aims to foster availability of data for use by increasing trust in data intermediaries and by strengthening data-sharing mechanisms across the EU. The DGA is important for KRAKEN for its requirements for data intermediation service providers, providers of services of data cooperatives, and data altruism organizations. Secondly, there is the Data Act (DA), which is still in the proposal phase and awaiting committee decision. The DA aims to ensure fairness in the allocation of value from data among actors in the data economy and to foster access to and use of data. It could be important for KRAKEN for its obligations for data consumers and the possibility of data subjects to receive and share data generated by products and services. Thirdly, we have the Digital Identity Regulation (eIDAS 2.0), which is also still in the proposal phase and awaiting committee decision. It amends the eIDAS Regulation and includes, for example, European Digital Identity Wallets (EDIW) and extra trust services. It may be important for KRAKEN in relation to self-sovereign identity (e.g., EDIW and electronic attestations of attributes). Fourthly, there is the Digital Services Act (DSA), which has been adopted by the Council and is awaiting entry into force. It aims to establish a harmonized horizontal framework for due diligence, accountability, and transparency for providers of intermediary services according to their role, size, and impact in the online sphere. The DSA may be important for KRAKEN considering its layered obligations for intermediary service providers, hosting providers, and online platforms, as well as its rules on liability for hosting providers. Lastly, the Digital Markets Act (DMA) has also been adopted by the Council and is awaiting entry into force. It aims to level the playing field for all digital companies by complementing existing competition rules and defining clear rules for big platforms. It is most likely not important for KRAKEN considering the high threshold for applicability.

The evaluation and validation of the ethical and legal requirements is based on the requirements formulated in D7.2 'Ethical and legal requirement specification'. The evaluation of requirements covers the different capacities in which KRAKEN may act. These include KRAKEN as a controller for account data, KRAKEN as a data exchange service provider, KRAKEN as a data analytics provider, and KRAKEN as a provider of an information society service. Not all the identified requirements (e.g., some organizational requirements) are applicable or were able to be implemented during the development phase of the KRAKEN platform. Consequently, before final adoption and exploitation of the platform, certain requirements should be revisited and considered at a later stage. The chapter on evaluation and validation also includes an update on the pilots that took place in 2021 and 2022, for which the KRAKEN consortium made changes to make use of fake personal data instead of real personal data where possible. As a result, many of the previously identified data protection risks have been mitigated.

Although not mandatory under the GDPR or soft-law guidelines, this deliverable also includes a lightweight development Data Protection Impact Assessment (DPIA). It is called *lightweight* because there is no definitive implementation of the system yet, which makes it difficult to conduct a complete DPIA for the KRAKEN end-product. It is a *development* DPIA because it signifies that it takes place

during the research and development phase of KRAKEN in order to identify and address risks in an early stage.

Lastly, it is important to also discuss some important topics and open issues that have been identified during the KRAKEN project. These include self-sovereign identity (SSI) and how it relates to KRAKEN, the role and implications of the use of blockchain, the roles and responsibilities under the GDPR, the anonymization of personal data, consent as a legal basis, and the monetization of personal data.

1 Introduction

1.1 Purpose of the document

The purpose of this document is to assess how far the ethical and legal requirements provided throughout the project have been taken into account within KRAKEN. It is part of Work Package 7 – 'Ethical and Legal compliance', which aims to provide KRAKEN consortium members with the necessary guidance for the implementation of the applicable ethical and legal requirements. As part of Task 7.2 – 'Ethical and Legal Analysis and Evaluation', this document includes an evaluation of the implementation of the ethical and legal requirements formulated in D7.2 'Ethical and legal requirement specification'. It furthermore includes policy recommendations based on the identified gaps and lessons learned.

1.2 Structure of the document

Chapter II of this deliverable provides an overview of upcoming legislation that may be relevant for the KRAKEN platform. This overview includes an analysis of the scope and accompanying obligations of the Data Governance Act, the Data Act Proposal, the Digital Identity Regulation Proposal, the Digital Services Act, and the Data Markets Act, as well as how these new rules could be relevant for the KRAKEN platform.

In Chapter III we provide an evaluation of the implementation of ethical and legal requirements formulated in in D7.2 'Ethical and legal requirement specification'. This evaluation is split up in different sections, where each section covers a different capacity of the KRAKEN platform. These include KRAKEN as a controller for account data, KRAKEN as a data exchange service provider, KRAKEN as a data analytics provider, and KRAKEN as a provider of an information society service. This chapter also includes a section with updated information relating to the KRAKEN pilots that took place in 2021 and 2022.

Chapter IV covers the lightweight development Data Protection Impact Assessment that was performed for the KRAKEN platform. This lightweight assessment focuses on several different scenarios and use-cases, including the risks and mitigating measures relating to account data, batch data, and data analytics.

In Chapter V we discuss the topic of self-sovereign identity and identity management and how it relates to the KRAKEN platform.

In Chapter VI, the final chapter, we discuss some open issues that we have identified during the KRAKEN project. Each issue, as well as how it relates to the KRAKEN project, is briefly described and analyzed. Open issues include the role and implications of blockchain, roles and responsibilities under the GDPR, the anonymization of personal data, consent as a legal basis, and the monetization of personal data.

2 Upcoming legislation

In the scope of the European data strategy[1] and digital services strategy[2], various new legislations have been proposed. This section will consider several legislative proposals and how far they might be relevant for KRAKEN.

2.1 The Data Governance Act

2.1.1 What is it and what does it aim for?

The Data Governance Act[3] (DGA) has been adopted on 30 May 2022, entered into effect on 23 June 2022 and will start to apply from 24 September 2023. It aims to foster the availability of data for use by increasing the trust in data intermediaries and by strengthening data-sharing mechanisms across the European Union (EU). As such, it is part of the European Data Strategy, creating an internal market for data, the European data space.[4] It is part of several complementing legislative proposals, and, in particular, close to the Data Act (see next section).[5]

The Regulation lays down[6]:

- conditions for the re-use, within the Union, of certain categories of data held by public sector bodies;
- a notification and supervisory framework for the provision of data intermediation services;
- a framework for voluntary registration of entities which collect and process data made available for altruistic purposes; and
- a framework for the establishment of a European Data Innovation Board.

While the provisions for public sector bodies are not relevant for KRAKEN, the second and the third point can have impact on KRAKEN.

The DGA covers personal as well as non-personal data and clearly notes that the General Data Protection Regulation (GDPR) will apply to any personal data processed in connection with the DGA.[7]

2.1.2 Would KRAKEN be a data intermediation service provider?

A data intermediation service provider (DISP) provides a data intermediation service. This service is defined as a service which aims to establish commercial relationships for the purposes of data sharing between an undetermined number of data subjects and data holders on the one hand and data users on the other, through technical, legal or other means, including for the purpose of exercising the rights of data subjects in relation to personal data (art. 2 (11) DGA). However, certain services are excluded

[1] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "A European strategy for data", COM/2020/66 final, 19.2.2020, https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1593073685620&uri=CELEX%3A52020DC0066, see also https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en#documents.

[2] European Commission, The Digital Services Act package, https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package.

[3] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act), *OJ* L 152/1, 3.6.2022." (*OJ* L 152/1, n.d.).

[4] Recital 2 DGA.

[5] Julie Baloup et al., "White Paper on the Data Governance Act," *SSRN Electronic Journal*, 2021, 5, https://www.ssrn.com/abstract=3872703.

[6] Art. 1 (1) DGA.

[7] Ibid., Art. 1 (3).

from the scope of this definition. These are: services that obtain data from data holders and aggregate, enrich or transform the data for the purpose of adding substantial value to it and license the use of the resulting data to data users, without establishing a commercial relationship between data holders and data users; services that focus on the intermediation of copyright-protected content; services that are exclusively used by one data holder in order to enable the use of the data held by that data holder, or that are used by multiple legal persons in a closed group, including supplier or customer relationships or collaborations established by contract, in particular those that have as a main objective to ensure the functionalities of objects and devices connected to the Internet of Things; and finally, data sharing services offered by public sector bodies that do not aim to establish commercial relationships.[8]

A *data holder* is defined as "a legal person, including public sector bodies and international organizations, or a natural person who is not a data subject with respect to the specific data in question, which, in accordance with applicable Union or national law, has the right to grant access to or to share certain personal data or non-personal data"[9]. A *data user* on the other hand is a "natural or legal person who has lawful access to certain personal or non-personal data and has the right, including under Regulation (EU) 2016/679 in the case of personal data, to use that data for commercial or non- commercial purposes"[10].

As KRAKEN aims to establish commercial relationships for the purpose of data sharing between an undetermined number of data providers, which entails data subjects and data holders, and data consumers, which are data users, it can be concluded that KRAKEN will be a data intermediary service provider. Since the analytics service still establishes a commercial relationship between data holders and data users, the exceptions do not apply. Therefore, the requirements stated in chapter III of the DGA will be applicable to KRAKEN.

2.1.3 Are Data Unions providing 'services of data cooperatives'?

Another newly introduced definition is the one of 'services of data cooperatives'. These are data intermediation services offered by an organizational structure constituted by data subjects, one-person undertakings or small and medium-sized enterprises (SMEs) who are members of that structure.[11] The main objectives of these data cooperatives are: to support its members in the exercise of their rights with respect to certain data, to exchange views on data processing purposes and conditions that would best represent the interests of its members in relation to their data, and to negotiate terms and conditions for data processing on behalf of its members before giving permission to the processing of non-personal data or before they consent to the processing of personal data. [12] Depending on how the data unions will be implemented, they might provide services of data cooperatives.

2.1.4 Could KRAKEN be a data altruism organization?

To be considered a data altruism organization, an organization needs to be registered in a public register at a competent authority for data altruism.[13] To be able to register it must be a legal person established pursuant to national law to meet objectives of general interest as provided for in national law, operate on a not-for-profit basis and be legally independent from any entity that operates on a for-profit basis and carry out data altruism activities. Data altruism means the voluntary sharing of data on the basis of the consent of data subjects to process personal data pertaining to them, or permissions of data holders to allow the use of their non-personal data without seeking or receiving a reward that

[8] Ibid., Art. 2 (11) (a) till (d).

[9] Ibid., Art. 2 (8).

[10] Ibid., Art. 2 (9).

[11] Ibid., Art. 2 (15).

[12] Ibid., Art. 2 (15).

[13] Ibid., Art. 17.

goes beyond compensation related to the costs that they incur where they make their data available for objectives of general interest as provided for in national law, where applicable.[14] Examples of such objectives are healthcare, combating climate change, improving mobility, facilitating the development, production and dissemination of official statistics, improving the provision of public services, public policy making or scientific research purposes in the general interest.[15] Furthermore, in order to register an organization must carry out its data altruism activities through a structure that is functionally separate from its other activities and comply with a rulebook which the Commission will provide via delegated acts.

2.1.5 Requirements for KRAKEN as data intermediation service provider

The requirements do not apply to data altruism organizations or other not-for-profit entities if their activities consist of seeking to collect data for objectives of general interest, made available by natural or legal persons on the basis of data altruism and they don't establish commercial relationships. However, as KRAKEN aims to establish commercial obligations, this exception does not apply. The requirements to be considered a data altruism organization are listed in section 2.1.7.

- Notification procedure (see further below);
- Fulfill the conditions of article 12 DGA:
    - don't use the data for other purposes than to put them at the disposal of data users;
    - provide data intermediation services through a separate legal person;
    - commercial terms, including pricing must be independent of whether or not other services of the DISP or a related entity are used;
    - any metadata collected on the person who uses the data intermediation service must be used only for the development of the data intermediation services (including also the detection of fraud or cybersecurity) and shall be made available to the data holders upon request;
    - facilitate the exchange of the data in the format in which it was received from a data subject or a data holder and convert the data into specific formats only (and provide an opt-out option, except in case the conversion has been mandated by law):
        - to enhance interoperability; or
        - if requested by the data user; or
        - if it was mandated by Union law; or
        - to ensure harmonization with international or European data standards.
    - may offer additional specific tools and services to data holders or data subjects for the specific purpose of facilitating the exchange of data, such as temporary storage, curation, conversion, anonymization and pseudonymization, as long as these tools are used only at the explicit request or approval of the data holder or data subject and third-party tools offered in that context are not used for other purposes;
    - must ensure that the procedure for access to its service is fair, transparent and non-discriminatory for both data subjects and data holders, as well as for data users, including with regard to prices and terms of service;
    - must have procedures in place to prevent fraudulent or abusive practices in relation to parties seeking access through its data intermediation services;

[14] Ibid., Art. 2 (16).
[15] Ibid., Art. 2 (16).

- in case of insolvency: must ensure a reasonable continuity of the provision of its data intermediation services and, where such data intermediation services ensure the storage of data, must have mechanisms in place to allow data holders and data users to obtain access to, to transfer or to retrieve their data and, where such data intermediation services are provided between data subjects and data users, to allow data subjects to exercise their rights;
- must take appropriate measures to ensure interoperability with other data intermediation services, inter alia, by means of commonly used open standards in the sector in which the DISP operates;
- must put in place adequate technical, legal and organizational measures in order to prevent the transfer of or access to non-personal data that is unlawful under Union law or the national law of the relevant Member State;
- must without delay inform data holders in the event of an unauthorized transfer, access or use of the non-personal data that it has shared;
- must take necessary measures to ensure an appropriate level of security for the storage, processing and transmission of non-personal data, and must further ensure the highest level of security for the storage and transmission of competitively sensitive information;
- if offering services to data subjects: must act in the data subjects' best interest where it facilitates the exercise of their rights, in particular by informing and, where appropriate, advising data subjects in a concise, transparent, intelligible and easily accessible manner about intended data uses by data users and standard terms and conditions attached to such uses before data subjects give consent;
- if providing tools for obtaining consent from data subjects or permissions to process data made available by data holders: must, where relevant, specify the third-country jurisdiction in which the data use is intended to take place and provide data subjects with tools to both give and withdraw consent and data holders with tools to both give and withdraw permissions to process data;
- must maintain a log record of the data intermediation activity.

KRAKEN normally already fulfills the more technical requirements.

2.1.6 Requirements for Data cooperatives

Data cooperatives, like other data intermediation services, have to notify their services according to art. 10 and follow the same notification procedure. Furthermore, they have to comply with the above-mentioned requirements for data intermediation services.

2.1.7 Requirements if KRAKEN would be a data altruism organization

In case KRAKEN would change its current approach and become a data altruism organization, it would need to comply with certain requirements. These requirements are listed in art. 20-22 DGA and cover transparency requirements, specific requirements to safeguard the rights and interests of data subjects and data holders, and a rulebook.

The transparency requirements entail that a data altruism organization has to keep full and accurate recording regarding:

- all natural or legal persons that were given the possibility to process data held by that recognized data altruism organization, and their contact details;
- the date or duration of the processing of personal data or use of non-personal data;
- the purpose of the processing as declared by the natural or legal person that was given the possibility of processing;
- the fees paid by natural or legal persons processing the data, if any.

Furthermore, the organization has to create an annual activity report which must be transmitted to the competent authority and which must entail information on the activities of the recognized data altruism organization and a description of the way in which the objectives of general interest for which data was collected have been promoted during the given financial year. Furthermore, it must include a list of all natural and legal persons that were allowed to process data it holds, including a summary description of the objectives of general interest pursued by such data processing and the description of the technical means used for it, and it must provide a description of the techniques used to preserve privacy and data protection. Finally, the report has to include a summary of the results of the data processing allowed by the recognized data altruism organization, where applicable, and information on sources of revenue of the recognized data altruism organization, in particular all revenue from allowing access to the data, and on expenditure.

The specific requirements to safeguard the rights and interests of data subjects and data holders consist of requirements regarding information, purpose specification, valid consent, security, notification of data breach and information on third-country jurisdictions.

To be more precise, the data altruism organization has to inform data subjects or data holders prior to processing:

- the objectives of general interest and, if applicable, the specified, explicit and legitimate purpose for which personal data is to be processed, and for which it permits the processing of their data by a data user; and
- the location of and the objectives of general interest for which it permits any processing carried out in a third country, where the processing is carried out by the recognized data altruism organization.

It should not use the data for other objectives than those of general interest for which the data subject or data holder allows the processing. The recognized data altruism organization shall not use misleading marketing practices to solicit the provision of data.

The data altruism organization should provide tools for obtaining consent from data subjects or permissions to process data made available by data holders. It shall also provide tools for easy withdrawal of such consent or permission.

Measures to ensure an appropriate level of security for the storage and processing of non-personal data that it has collected based on data altruism should be taken.

In the event of any unauthorized transfer, access or use of the non-personal data it has shared, it has to inform the data holders without delay. Though not mentioned in the DGA, as it is an obligation under the GDPR, the same obligation arises with regard to personal data.

Where the recognized data altruism organization facilitates data processing by third parties, including by providing tools for obtaining consent from data subjects or permissions to process data made available by data holders, it shall, where relevant, specify the third-country jurisdiction in which the data use is intended to take place.

Finally, it is intended that the data altruism organizations will comply with a rulebook. This rulebook will give guidance on appropriate information requirements, so that before a consent or permission for data altruism is given, it is ensured that data subjects and data holders are provided with sufficiently detailed, clear and transparent information regarding the use of data, the tools for giving and withdrawing consent or permission, and the measures taken to avoid misuse of the data shared with the data altruism organization. The rulebook shall also include appropriate technical and security requirements to ensure the appropriate level of security for the storage and processing of data, as well as for the tools for giving and withdrawing consent or permission; communication roadmaps taking a multi-disciplinary approach to raise awareness of data altruism, of the designation as a 'data altruism organization recognized in the Union' and of the rulebook among relevant stakeholders, in particular data holders and data subjects that would potentially share their data; and finally, recommendations on relevant interoperability standards.

This rulebook is not yet ready, but it should be prepared by the Commission in close cooperation with data altruism organizations and relevant stakeholders, and be adopted in the form of a delegated act.

2.1.8 How does the notification/registration procedure work?

Data intermediation service: **Notification**

When intending to provide data intermediation services a notification must be submitted to the competent authority of the Member State in which the provider has its main establishment.[16] The activities may only be started after submitting the notification, but it entitles the DISP to provide data intermediation services in all Member States.[17] Fees may be charged for the notification, but may also be discounted or waived for SMEs and start-ups.[18]

The notification must include:

- the name of the DISP;
- the DISP's legal status, form, ownership structure, relevant subsidiaries and, where the data intermediation services provider is registered in a trade or other similar public national register, registration number;
- the address of the DISP's main establishment in the Union, if any, and, where applicable, of any secondary branch in another Member State or that of the legal representative;
- a public website where complete and up to date information on the DISP and the activities can be found, including as a minimum the information above and a description of the provided services and under which category the service falls (a non-personal data exchange service (art. 10 (a) DGA), a personal data exchange service (art. 10 (b) DGA) or a data cooperative service (art. 10 (c) DGA));
- contact persons and contact details;
- a description of the data intermediation service the DISP intends to provide, and an indication of the categories under which such data intermediation service falls;
- the estimated date for starting the activity, if different from the date of the notification.

In case any of the provided information changes, the DISP will have to notify the competent authority within 14 days of the date of change.[19]

One week after a duly and fully completed notification, the competent authority will issue a standardized declaration at the request of the DISP. This declaration confirms that the DISP has submitted the complete notification.[20] Furthermore, a DISP can request the competent authority to confirm that it complies with the notification obligation and the requirements of article 12 DGA. When

[16] Ibid., Art. 11 (1) and (2).

[17] Ibid., Art. 11 (4) and (5).

[18] Ibid., Art. 11 (11).

[19] Ibid., Art. 11 (12).

[20] Ibid., Art. 11 (8).

receiving such a confirmation, the DISP may use the label 'Data intermediation services provider recognized in the Union' as well as a common logo.[21] In case a DISP will cease its activities, it must notify the competent authority within 15 days.[22]

The Commission will keep and regularly update a public register of all data intermediation services providing their services in the Union, based upon the information from the competent authorities.[23] Information about changes of the provided information or if a DISP ceases its activities must be provided to the Commission without delay by electronic means to update the public register.[24]

Data cooperation: **Notification**

The same as for data intermediation services.

Data altruism organization: **Registration**

A data altruism organization must register in a public national register of recognized data altruism organizations in order to be recognized as a data altruism organization. In order to qualify for such a registration, it must carry out data altruism activities, be a legal person established to meet objectives of general interest according to national law, operate on a not-for-profit basis and be legally independent from any entity that operates on a for-profit basis and carry out the data altruism activities through a structure that is functionally separate from its other activities.[25] Finally, at the latest 18 month after the rulebook mentioned above has entered into force, the organization needs to comply with it.[26] If these requirements are met, than the entity may submit an application for registration in the public national register of recognized data altruism organizations in the Member State in which it is established or has its main establishment.

2.1.9 Who is the competent authority?

Each Member State can designate one or more competent authorities to carry out the tasks related to the notification procedure for data intermediation services.[27] Each Member State shall also designate one or more competent authorities who are responsible for its public national register of recognized data altruism organizations.[28] By 24 September 2023 the Member States will inform the Commission of the identity of these competent authorities.[29]

2.1.10 What if a DISP does not comply with the DGA requirements?

The competent authorities will monitor and supervise the compliance with the requirements and for that they may request all the information that is necessary to verify compliance.[30] In case a DISP is found not to comply with the requirements, it will be notified and gets the opportunity to state its views.[31] The competent authority can require the cessation of the infringement within a reasonable time limit, or in case of a serious infringement, immediately.[32] The authority has the power to impose financial penalties and initiate legal proceedings for the imposition of fines, can require a delay of the

[21] Ibid., Art. 11 (9).
[22] Ibid., Art. 11 (13).
[23] Ibid., Art. 11 (10).
[24] Ibid., Art. 11 (14).
[25] Ibid., Art. 18.
[26] Ibid., Art. 18 (e).
[27] Ibid., Art. 13 (1).
[28] Ibid., Art. 23.
[29] Ibid., Art. 13 (1) and Art. 23 (2).
[30] Ibid., Art. 14 (1) and (2) and Art. 24 (1) and (2).
[31] Ibid., Art. 14 (3).
[32] Ibid., Art. 14 (4).

beginning or a suspension of the provision of the data intermediation service, and can require the cessation of the provision of the data intermediation service.[33]

2.1.11 European data altruism consent form

It is planned that the European Commission will adopt implementing acts which establish and develop a European data altruism consent form.[34] This will be done with consultation of the European Data Protection Board (EDPB), advice of the European Data Innovation Board and involvement of relevant stakeholders. The goal is that this form will allow the collection of consent or permission across Member States in a uniform format and shall use a modular approach in order to allow for the customization for specific sectors or different purposes.[35] In case of personal data, the form shall comply with the requirements of the GDPR and it will be available in a manner that it will be on the one hand easily understandable also if it would be printed on paper and on the other it will also be in an electronic, machine-readable form.[36]

2.2 The Data Act Proposal

2.2.1 What is it and what does it aim for?

The European Commission published in February 2022 as part of the European Strategy for data[37] its proposal for a Regulation of the European Parliament and of the Council on harmonized rules on fair access to and use of data, shortly referred to as Data Act (DA). The legislative process is currently still ongoing and the analysis here is based on the original European Commission proposal.

The aim of the Data Act is to ensure fairness in the allocation of value from data among actors in the data economy and to foster access to and use of data. The specific objectives, as outlined by the explanatory memorandum are:[38]

- facilitate access to and the use of data by consumers and businesses, while preserving incentives to invest in ways of generating value through data;
- provide for the use by public sector bodies and Union institutions, agencies or bodies of data held by enterprises in certain situations where there is an exceptional data need;
- facilitate switching between cloud and edge services;
- Put in place safeguards against unlawful data transfer without notification by cloud service providers; and
- provide for the development of interoperability standards for data to be reused between sectors.

2.2.2 What is important for KRAKEN?

Aspects of the proposal that could be relevant for KRAKEN are the provision of the development of interoperability standards for data to be reused between sectors (current chapter 8) and the facilitation of access to and use of data (current chapters 2 and 3). This provides data subjects a possibility to receive and share data generated by products or services they use, and it is therefore in that regard relevant in the scope of the KRAKEN services. It also includes a right to share data with

[33] Ibid., Art. 14 (4).
[34] Ibid., Art. 25 (1).
[35] Ibid., Art. 25 (1) and (2).
[36] Ibid., Art. 25 (3) and (4).
[37] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions, "A European strategy for data", 19 of February 2020, COM (2020) 66 final.
[38] Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act)," Pub. L. No. COM(2022) 68 final (23.3.2022), 3.

third parties (current art. 5 DA), whereby gatekeeper services (as specified in the Data Markets Act (DMA)) are currently excluded from the status as third party. Furthermore, the proposal includes obligations for the data consumer.

The current art. 28 DA specifies essential requirements regarding interoperability for operators of data spaces, however, these operators are currently not defined in the proposal.

Finally, the current art. 30 DA defines essential requirements regarding smart contracts for data sharing which is in particular relevant for KRAKEN. Though this might still change during the legislative process, currently the one who uses smart contracts for others (e.g., vendor of an application using smart contracts) in the context of an agreement to make data available has to make sure that the smart contract is robust, a mechanism exists to terminate the continued execution of transactions, and in such a case provide the possibility to archive transactional data, the smart contract logic and code to keep a record of the past operations, and use rigorous access control mechanisms at the governance and smart contract layers.[39] The fulfilment of the requirements must be confirmed by a conformity assessment and then an EU declaration of conformity, which will make the vendor responsible for compliance with the requirements.[40]

It is intended that harmonized standards will be drafted and published in the Official Journal of the European Union, but until then the Commission may by way of implementing acts, adopt common specification regarding the essential requirements.[41]

Current art. 6 DA specifies certain obligations for data consumers, such as that it might process the data only for the purposes and under the conditions agreed with the user and subject to the rights of the data subject, and shall delete the data when they are no longer necessary for the agreed purpose. Furthermore, the data consumer is forbidden to: 1) coerce, deceive or manipulate the user in any way, by subverting or impairing the autonomy, decision-making or choices of the user, including by means of a digital interface with the user; 2) use the data it receives for the profiling of natural persons, unless it is necessary to provide the service requested by the user; 3) make the data available it receives to another third party, in raw, aggregated or derived form, unless this is necessary to provide the service requested by the user; 4) make the data available it receives to an undertaking providing core platform services for which one or more of such services have been designated as a gatekeeper; 5) use the data it receives to develop a product that competes with the product from which the accessed data originate or share the data with another third party for that purpose; and 6) prevent the user, including through contractual commitments, from making the data it receives available to other parties.

2.3 The Digital Identity Regulation Proposal

2.3.1 What is it and what does it aim for?

In June 2021, the European Commission published the Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity.[42] The proposed Digital Identity Regulation (eIDAS 2.0) would amend the eIDAS Regulation[43] as the evaluation of the eIDAS Regulation showed that the eIDAS Regulation fell short in certain new market demands as it is focused on the public sector. It is currently

[39] Art. 30 (1) DA.

[40] Ibid., Art. 30 (2) and (3).

[41] Ibid., Art. 30 (4) till (6).

[42] Proposal for a Regulation of the European Parliament and of the Council Amending Regulation (EU) No 910/2014 as Regards Establishing a Framework for a European Digital Identity” (European Commission 2021/0136 (COD), 3.6.2021), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0281.

[43] 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,” Pub. L. No. OJ L 257/73, OJ L 257/73 (28.8.2014).

awaiting Committee decision; accordingly the information below might change during the legislative process.

The focus is on cross-border use, for which the proposed Digital Identity Regulation aims to provide access to highly secure and trustworthy electronic identity solutions, on which public and private services can rely on.[44] It also aims to empower natural and legal persons to use digital identity solutions, linking these solutions to a variety of attributes while providing that these solutions allow for only sharing of identity data that the specific service actually needs.[45] Finally, it also aims to improve the acceptance of qualified trust services in the EU and create equal conditions for providing them. [46]

It aims to do this by amending the eIDAS Regulation, in particular by introducing European Digital Identity Wallets and provisions relating to them, and by introducing additional trust services (electronic attestations of attributes, qualified electronic archiving and electronic ledgers).

2.3.2 What is important for KRAKEN?

For KRAKEN, the provisions on European Digital Identity Wallets (EDIW), electronic attestation of attributes, electronic signatures and electronic ledgers are the most relevant.

European Digital Identity Wallet (EDIW): EDIW are defined as ‘a product and service that allows the user to store identity data, credentials and attributes linked to his/her identity, to provide them to relying parties on request and to use them for authentication, online and offline, for a service in accordance with Article 6a; and to create qualified electronic signatures and seals”[47] that are considered as electronic identification means[48]. The European Commission foresees a trust mark for EDIWs, to indicate that a wallet has been issued in accordance with the Regulation. EDIWs can only be issued by a Member State or under a mandate of a Member State or independently, but recognized by a Member State.[49] It must be free of charge for natural persons and issued under a notified electronic identification scheme with a level of assurance ‘high’.

The KRAKEN self-sovereign identity (SSI) system currently uses the eIDAS system to create an e-ID for the Legal Identity Manager. In principle, it would be possible to use in future the European Digital identity Wallets for this purpose. In such a case, the KRAKEN provider would become a relying party, and art. 6b of the amended eIDAS Regulation would be applicable. Accordingly, the KRAKEN provider would need to communicate to the Member State where the KRAKEN provider is established that they intend to rely upon EDIWs and what the intended use is, to ensure compliance with the requirements set out in Union law of national law for the provision of specific services.[50] It is furthermore proposed that Member States will implement a common mechanism for the authentication of relying parties.[51] For this the European Commission would provide technical and operational specifications in an implementing act within 6 months after the Digital Identity Regulation would enter into force.[52] The relying party would be responsible for carrying out the procedure for authenticating person identification data and electronic attestations of attributes coming from the EDIW.[53]

[44] Explanatory Memorandum “Proposal for a Regulation of the European Parliament and of the Council Amending Regulation (EU) No 910/2014 as Regards Establishing a Framework for a European Digital Identity,” 1.

[45] Explanatory Memorandum “Proposal for a Regulation of the European Parliament and of the Council Amending Regulation (EU) No 910/2014 as Regards Establishing a Framework for a European Digital Identity,” 1.

[46] Explanatory Memorandum “Proposal for a Regulation of the European Parliament and of the Council Amending Regulation (EU) No 910/2014 as Regards Establishing a Framework for a European Digital Identity,” 1.

[47] Art. 3 (42) eIDAS2.0.

[48] Ibid., Art. 3 (2).

[49] Ibid., Art. 6a (2).

[50] Ibid., Art. 6b (1).

[51] Ibid., Art. 6b (2).

[52] Ibid., Art. 6b (4).

[53] Ibid., Art. 6b (3).

Electronic attestation of attributes: Electronic attestation of attributes is defined as "an attestation in electronic form that allow the authentication of attributes"[54], whereby attributes are defined as a "feature, characteristic or quality of a natural or legal person or of an entity, in electronic form"[55]. The proposed Digital Identity Regulation would add an additional section in the eIDAS Regulation. The legal effects of electronic attestation of attributes are specified, which are similar to the legal effects of electronic signatures, and the requirements for qualified attestations of attributes.[56] A qualified electronic attestation of attributes would have the same legal effect as lawfully issued attestations in paper form.[57]

Electronic signatures: While the general provisions of electronic signatures remain largely the same, the Digital Identity Regulation adds the management of remote electronic signature and seal creation devices to the definition of trust services.[58] Remote qualified signature creation device is defined as "a qualified electronic signature creation device where a qualified trust service provider generates, manages or duplicates the electronic signature creation data on behalf of a signatory"[59](art. 3 (23a) eIDAS2.0). This may only be done by a qualified trust service provider[60]. The Digital Identity Regulation proposal also introduces the requirements for a qualified service for the management of remote electronic signature creation devices into the eIDAS Regulation.[61]

The proposed Digital Identity Regulation obliges the European Commission to establish reference numbers of standards for qualified certificates for electronic signatures, for the validation of qualified electronic signatures and for the qualified preservation service for qualified electronic signatures, within 12 months after entry into force of the Regulation.[62]

Electronic ledgers: Another completely new trust service which the Digital Identity Regulation proposal would introduce in the eIDAS Regulation is the *recording of electronic data into an electronic ledger.*[63] An electronic ledger is defined as "a tamper proof electronic record of data, providing authenticity and integrity of the data it contains, accuracy of their date and time, and of their chronological ordering".[64] Like for other trust services, also for electronic ledgers a normal version and a qualified version is introduced. The requirements for qualified electronic ledgers are currently the following: they must be created by one or more qualified trust service provider or providers and ensure the uniqueness, authenticity and correct sequencing of data entries recorded in the ledger. Furthermore, they must ensure the correct sequential chronological ordering of data in the ledger and the accuracy of the date and time of the data entry, and record data in such a way that any subsequent change to the data is immediately detectable.[65] The legal effects of electronic ledgers are depending on this qualification. When used as evidence in legal proceedings, for a normal electronic ledger the non-discrimination principle applies. This means that it must not be denied legal effect and admissibility only because it is in an electronic form or because it does not meet the requirements for a qualified electronic ledger.[66] For a qualified electronic ledger the proposal currently defines the legal effect as "the presumption of

[54] Ibid., Art. 3 (44).
[55] Ibid., Art. 3 (43).
[56] Ibid., Art. 45a and 45c.
[57] Ibid., Art. 45a (2).
[58] Ibid., Art. 3 (16).
[59] Ibid., Art. 3 (23a).
[60] Ibid., Art. 29 (1a).
[61] Ibid., Art. 29a.
[62] Ibid., Art. 28 (6), Art. 32 (3) and Art. 34 (3).
[63] Ibid., Art. 3 (16).
[64] Ibid., Art. 3 (53).
[65] Ibid., Art. 45i (1).
[66] Ibid., Art. 45h (1).

the uniqueness and authenticity of the data it contains, of the accuracy of their date and time, and of their sequential chronological ordering with the ledger".[67]

2.4 The European Health Data Space Proposal

2.4.1 What is it and what does it aim for?

The Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space[68] is part of the European strategy of data. It is the first proposal regarding a domain-specific European Data Space. Its general objective is to ensure that natural persons in the EU have increased control over their electronic health data, while at the same time ensuring a legal framework allowing researchers, innovators, policymakers and regulators to access relevant electronic health data.[69] The Commission adopted the proposal on 4.5.2022, and the legislative process is currently still ongoing.

2.4.2 What is important for KRAKEN?

This Regulation, once adopted, will be relevant for the KRAKEN health data use-case. In particular, the current chapter IV regarding the secondary use of electronic health data can be relevant. However, the access to the data is expected to be granted through Health Data Access Bodies.

Electronic health data is in the current proposal defined as personal and non-personal electronic health data.[70] Personal electronic health data means data processed in electronic form, concerning health and genetic data as defined by the GDPR, as well as data referring to determinants of health, or data processed in relation to the provision of healthcare services.[71] Non-personal electronic form means data concerning health and genetic data in electronic format that are not personal data.[72]

Member States can establish one or more Health Data Access Bodies. These Health Data Access Bodies are responsible for granting access to electronic health data for secondary use. The Health Data Access Bodies may be either new public sector bodies, or existing public sector bodies or internal services of public sector bodies.[73] The proposal also includes provisions on health data quality and utility for secondary use. This entails that health data access bodies inform the data users about the available datasets and their characteristics through a metadata catalogue.[74] The minimum information that needs to be provided, will be defined by the European Commission in implementing acts. [75] Furthermore, the datasets may have a Union data quality and utility label. [76]

The proposal is currently still at the beginning of the legislative process, therefore the provisions might still change considerably.

[67] Ibid., Art. 45h (2).

[68] Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space, 3.5.2022, COM(2022) 197 final, https://eur-lex.europa.eu/resource.html?uri=cellar:dbfd8974-cb79-11ec-b6f4-01aa75ed71a1.0001.02/DOC_1&format=PDF.

[69] Health Data Space Proposal, 1.

[70] Ibid., Art. 2 (2) (c).

[71] Ibid., Art. 2 (2) (a).

[72] Ibid., Art. 2 (2) (b).

[73] Ibid., Art. 36.

[74] Ibid., Art. 55 (1).

[75] Ibid., Art. 55 (2).

[76] Ibid., Art. 56 (1).

2.5 The Digital Services Act

2.5.1 What is it and what does it aim for?

The Digital Services Act (DSA), together with the Digital Markets Act (DMA), is part of a legislative package governing digital services in the EU. The term 'digital service' is quite broad and covers a range of online services such as websites, online platforms, and infrastructure services, including online marketplaces, social media, cloud services, content sharing-platforms, search engines, app stores, etc. The legislative initiative aims to foster safety and openness in the digital space by promoting the fundamental rights of all users and levelling the playing field to stimulate innovation, growth, and competitiveness. The package responds to the need to address the consequences and concerns resulting from the expanding development of digital services in the EU; including issues such as the exchange of illegal goods, services, and content online, as well as the spread of disinformation and the ever-growing market position of very large online platforms.[77]

The Council has adopted the DSA on 4 October 2022. It will become directly applicable in the EU fifteen months after its entry into force, which occurs twenty days after its publication in the Official Journal of the European Union.[78] The DSA establishes a harmonized horizontal framework for accountability and transparency for providers of intermediary services according to their role, size, and impact in the online sphere.[79] It complements sector-specific legislation such as the Audiovisual Media Services Directive and the Directive on Copyright in the Digital Single Market and does not replace the existing e-Commerce Directive[80] and Platform-to-Business Regulation[81], but rather incorporates the existing rules exempting online intermediaries from liability under specific conditions.[82]

2.5.2 Scope of application

The DSA applies to all providers of intermediary services that offer their services to recipients in the EU. Consequently, all recipients of intermediary services that have their place of establishment or residence in the EU will benefit from the DSA, irrespective of the place of establishment of the providers of those intermediary services.[83] The DSA, like the e-Commerce Directive, also specifies which services fall under its scope by categorizing intermediary services into three groups:

- *mere conduit services*: consist of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network;
- *cashing services*: consist of the transmission in a communication network of information provided by a recipient of the service, involving the automatic, intermediate and temporary

[77] European Commission, The Digital Services Act package, https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package.

[78] Art. 74 of the Position of the European Parliament adopted at first reading on 5 July 2022 with a view to the adoption of Regulation (EU) 2022/… of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC (hereafter 'the DSA Proposal'); European Commission, The Digital Services Act package, https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package; and European Council and Council of the European Union, Digital services package, https://www.consilium.europa.eu/en/policies/digital-services-package/.

[79] European Council and Council of the European Union, Digital services package, https://www.consilium.europa.eu/en/policies/digital-services-package/.

[80] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce').

[81] Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services.

[82] European Parliament, Briefing: EU Legislation in Progress: Digital services act, https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689357/EPRS_BRI(2021)689357_EN.pdf, 4.

[83] Art. 1a (1) DSA Proposal.

storage of that information, performed for the sole purpose of making more efficient the information's onward transmission to other recipients upon their request;

- *hosting services*: consist of the storage of information provided by, and at the request of, a recipient of the service.[84]

In addition to these three categories of intermediary services, for which the DSA establishes a set of responsibilities and obligations, it lays down additional obligations for a specific subcategory of hosting services: online platforms. Online platforms (e.g., online marketplaces, apps stores, social media, content sharing websites, collaborative economy platforms, etc.)[85] are hosting services that do not merely store information at the request of a recipient of the service, but also disseminate that information to the public.[86] A dissemination to the public means that the online platform makes available information, at the request of the recipient of the service who provided the information, to a potentially unlimited number of third parties.[87]

Lastly, the DSA also recognizes the existence of very large online platforms (VLOPs) that have a widespread impact on society and pose particular risks in the dissemination of illegal content and societal harms, especially considering their influence on public discourse and online behaviour.[88] An online platform qualifies as a VLOP if that platform reaches 45 million or more average monthly active recipients in the EU (10% or more of the total EU population) calculated over a period of six months and has been designated as a VLOP.[89] The qualification as a VLOP incurs the highest standard of due diligence and additional stringent obligations to manage systemic risks.

2.5.3 Layered obligations

Chapter III of the DSA establishes a set of layered and asymmetric obligations covering the due diligence of service providers and the transparency and safety of the online environment. The DSA distinguishes four types of actors or services with cumulative layered obligations: *intermediary services*, *hosting services*, *online platforms*, and *VLOPs*.

2.5.3.1 General provisions: liability exemptions

Similar to the eCommerce Directive, Chapter II of the DSA sets out liability exemptions for mere conduit[90], cashing[91], and hosting[92] service providers. It also reiterates that no general obligation to monitor the information which they transmit or store, nor actively to seek facts or circumstances indicating illegal activity shall be imposed on those providers.[93] It is important to note that providers of intermediary services may conduct voluntary own-initiative investigations and take measures in good faith and in a diligent manner without being deemed ineligible for the liability exemptions.[94]

Providers of intermediary services should, upon receipt of an order to act against illegal content, issued by the relevant national judicial or administrative authorities, inform without undue delay the relevant authorities of any follow-up given to the order, specifying if and when the order was applied.[95]

[84] Ibid., Art. 2 (f).

[85] European Council and Council of the European Union, Digital services package, https://www.consilium.europa.eu/en/policies/digital-services-package/.

[86] Art. 2 (h) DSA Proposal.

[87] Ibid., Recital 14 and Art. 2 (i).

[88] Ibid., Recital 43, 53, and 56; and European Parliament, Briefing: EU Legislation in Progress: Digital services act, https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689357/EPRS_BRI(2021)689357_EN.pdf, 4.

[89] Recital 54 and Art. 25 DSA Proposal.

[90] Ibid., Art. 3.

[91] Ibid., Art. 4.

[92] Ibid., Art. 5.

[93] Ibid., Art. 7.

[94] Ibid., Art. 6.

[95] Ibid., Art. 8.

Similarly, they must also, upon receipt of an order to provide information about one or more specific recipients of the service, inform without undue delay the relevant authorities of its receipt, the effect given to the order, specifying if and when the order was applied.[96]

2.5.3.2 First layer: intermediary services

Section I of Chapter III lays down the first layer of obligations and responsibilities applicable to all intermediary service providers (i.e., all mere conduit, cashing, and hosting service providers).

Firstly, providers of intermediary services are obliged to designate a single point of contact in order to facilitate communication with Member States' authorities and other relevant authorities. Such a point of contact must also be established for communication with the recipients of their service. The information relating to their single points of contact must be made public, easily accessible, and kept up to date.[97] Providers that offer intermediary services in the EU but are established outside of the EU must also designate a legal representative in one of the Member States where their services are offered. The information relating to the legal representative must be made public, easily accessible, accurate, and kept up to date.[98]

Secondly, the DSA stipulates that providers of intermediary services must include information on any restrictions that they impose in relation to the use of their service in respect of information provided by the recipients of the service, in their terms and conditions. This includes information on policies, procedures, measures, and tools employed for the purpose of content moderation (incl. algorithmic decision-making and human review), as well as rules relating to their internal complaint handling system. This information must be made publicly available, easily accessible, and presented in clear, plain, intelligible, user-friendly, and unambiguous language.[99]

Finally, intermediary service providers must publish, at least once a year, clear and easily comprehensible reports on any content moderation they engaged in during the relevant period. These reports must be publicly available and easily accessible. It is important to note that this obligation does not apply to intermediary services that qualify as micro or small enterprises and which are not considered VLOPs as defined under Article 25 of the DSA.[100] Commission Recommendation 2003/361/EC defines a small enterprise as "*an enterprise which employs fewer than 50 persons and whose annual turnover and/or annual balance sheet total does not exceed EUR 10 million*" and a microenterprise as "*an enterprise which employs fewer than 10 persons and whose annual turnover and/or annual balance sheet does not exceed EUR 2 million*".[101] As a result, intermediary service providers that are not considered a VLOP while employing fewer than 50 persons and with an annual turnover and/or balance sheet that does not exceed EUR 10 million do not fall under the reporting obligation.

2.5.3.3 Second layer: hosting services

Section II of Chapter III sets out the second layer of obligations and responsibilities applicable to one specific type of intermediary service providers: hosting service providers.

Firstly, hosting service providers should implement notice and action mechanisms that enable third parties to notify the presence of alleged illegal content. These mechanisms should be easy to access, user-friendly, and allow for the submission of notices exclusively by electronic means. Such notices are considered to give rise to actual knowledge or awareness for the purpose of the liability exemption in

[96] Ibid., Art. 9.

[97] Ibid., Art. 10 (1) and (2) and Art. 10a.

[98] Ibid., Art. 11 (1) and (4).

[99] Ibid., Art. 12 (1).

[100] Ibid., Recital 39 and Art. 13 (1) and (2).

[101] Art. 2 of the Annex to the Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises.

Article 5 where they allow a diligent provider of hosting services to identify the illegality of the relevant activity or information without a detailed legal examination.[102]

Secondly, in case hosting service providers restrict, remove or disable access to content they should provide a clear and specific statement of reasons to any affected recipients of the service. This obligation also applies if the hosting service provider restricts, suspends, or terminates monetary payments, the provision of the service in whole or in part, or the recipient's accounts.[103]

Finally, in case a provider of hosting services becomes aware of any information giving rise to a suspicion that a criminal offence involving a threat to the life or safety of a person or persons has taken place, is taking place or is likely to take place, it shall promptly inform the relevant authorities of the Member State.[104]

2.5.3.4 Third layer: online platforms

Section III of Chapter III establishes the third layer of obligations and responsibilities applicable to one specific type of hosting service providers: providers of online platforms.

As an exemption, the obligations and responsibilities under this section, with the exception of Article 23 (3), do not apply to providers of online platforms that qualify as micro or small enterprises and which are not considered VLOPs as defined under Article 25 of the DSA.[105]

Firstly, providers of online platforms must establish an easily accessible, user-friendly, and effective internal complaint-handling system that allows recipients of their service to lodge complaints against decisions taken upon the receipt of a notice or against decisions taken on the ground that the information provided by the recipients is illegal content or incompatible with its terms and conditions.[106] Recipients of the online platform service addressed by the decisions mentioned in this paragraph are entitled to select any out-of-court dispute settlement body that has been certified in accordance with Article 18 of the DSA in order to resolve disputes relating to those decisions.[107]

Secondly, the DSA introduces the concept of trusted flaggers; entities appointed by the Digital Services Coordinators of Member States with particular expertise and competence in detecting, identifying and notifying illegal content. Providers of online platforms should ensure that notices submitted by trusted flaggers are processed and decided upon with priority and without undue delay.[108] In order to protect against misuse, providers of online platforms should suspend the provision of their services to recipients that frequently provide manifestly illegal content. They should also suspend the processing of notices and complaints submitted through the notice and action mechanisms and internal complaint-handling systems by entities that frequently submit notices or complaints that are manifestly unfounded.[109]

Thirdly, providers of online platforms are subject to additional transparency obligations relating to the reporting obligation applicable all intermediary service providers. This includes information on the disputes submitted to the out-of-court dispute settlement bodies as well as information on the suspensions imposed as a result of misuse as mentioned in the previous paragraph. Providers of online platforms must also publish in a publicly available section of their online interface information on the average monthly active recipients of their service in the EU, calculated as an average over the period

[102] Art. 14 (1) and (3) DSA Proposal.
[103] Ibid., Art. 15a (1).
[104] Ibid., Art. 15.
[105] Ibid., Recital 43 and Art. 16.
[106] Ibid., Art. 17 (1) and (2).
[107] Ibid., Art. 18 (1).
[108] Ibid., Art. 19 (1) and (2).
[109] Ibid., Art. 20 (1) and (2).

of the past six months.[110] This last information obligation relates to the potential qualification of an online platform as a VLOP as defined under Article 25 of the DSA.

Fourthly, the DSA obliges providers of online platforms to refrain from designing, organizing or operating their online interfaces in a way that deceives, manipulates or otherwise materially distorts or impairs the ability of recipients to make free and informed decisions. Prohibited practices include giving more prominence to certain choices when asking the recipients for a decision, repeatedly requesting the recipients to make a choice where such a choice has already been made and making the procedure of terminating a service more difficult than subscribing to it.[111] In case providers of online platforms make use of recommender systems[112], they must set out in their terms and conditions, in plain and intelligible language, the main parameters used in their recommender systems, as well as any options to modify or influence those parameters.[113] In a similar vein, providers of online platforms that present advertising on their online interfaces must ensure that recipients can identify in a clear, concise and unambiguous manner and in real time: that the information presented is an advertisement, the entity on whose behalf the advertisement is presented, the entity who paid for the advertisement, and meaningful information about the main parameters used to determine the recipients to whom the advertisement is presented and where applicable about how to change those parameters. In addition, it is prohibited for providers of online platforms to present advertising to recipients based on profiling using special categories of personal data.[114] Moreover, they should also protect minors by implementing appropriate and proportionate measures to ensure a high level of privacy, safety, and security of minors. As a more stringent obligation, it is therefore prohibited to present advertising to recipients based on profiling using personal data of the recipient when they are aware with reasonable certainty that the recipient is a minor.[115]

Lastly, there also exist provisions relating to providers of online platforms that allow consumers[116] to conclude distance contracts with traders[117], such as online marketplaces. In order to make use of those services, traders must first provide specific information (e.g., contact details, an identification document, payment account details, etc.) to the provider of the online platform. It is then up to the service provider to make best efforts to assess whether that information is reliable and complete, using any freely accessible official online database or interface made available by the Member States or EU or through requests to the trader to provide supporting documents from reliable source. The relevant information must also be made available to recipients, for example on the product listing.[118] It is also important that the online platforms that fall under the obligations described in this paragraph design and organize their interface in a way that enables traders to comply with the obligations regarding pre-contractual information, compliance, and product safety.[119] Moreover, providers of these online platforms should make reasonable efforts to randomly check whether the content offered has been identified as being illegal in any official, freely accessible and machine-readable online database or

[110] Ibid., Art. 23 (1) and (2).

[111] Ibid., Art. 23a.

[112] Art. 2 (o) DSA Proposal defines a recommender system as "*a fully or partially automated system used by an online platform to suggest or prioritise in its online interface specific information to recipients of the service, including as a result of a search initiated by the recipient of the service or otherwise determining the relative order or prominence of information displayed*".

[113] Ibid., Recital 52c and Art. 24a (1).

[114] Ibid., Art. 24 (1) and (3).

[115] Ibid., Art. 24b (1) and (1b).

[116] Art. 2 (c) DSA Proposal defines consumer as "*any natural person who is acting for purposes which are outside his or her trade, business, craft, or profession*".

[117] Art. 2 (e) DSA Proposal defines trader as "*any natural person, or legal person irrespective of whether privately or publicly owned, who is acting, including through any person acting in his or her name or on his or her behalf, for purposes relating to his or her trade, business, craft or profession*".

[118] Ibid., Art. 24c (1), (2) and (6).

[119] Ibid., Art. 24d (1).

interface.[120] In case the provider of such an online platform becomes aware, irrespective of the means used, of illegal content offered by a trader to consumers in the EU, it must inform the consumers that purchased the content during the last six months about the illegality, the identity of the trader, and any relevant means of redress.[121]

2.5.3.5 Fourth layer: very large online platforms (VLOPs)

Section IV of Chapter III lays down the fourth layer of obligations and responsibilities applicable to VLOPs.

As mentioned before, an online platform qualifies as a VLOP if that platform reaches 45 million or more average monthly active recipients in the EU (10% or more of the total EU population) calculated over a period of six months and has been designated as a VLOP.[122] The qualification as a VLOP incurs the highest standard of due diligence and additional stringent obligations to manage systemic risks.

The obligations and responsibilities applicable to VLOPs will not be described in detail since they are not as relevant for the KRAKEN platform.

Firstly, providers of VLOPs must diligently identify, analyse, and assess any systemic risks stemming from the design, including algorithmic systems, functioning and use made of their services. For these purposes, they must conduct yearly risk assessments and take reasonable, proportionate, and effective mitigation measures tailored to the specific systemic risks identified.[123] VLOPs must also implement crisis response mechanisms where extraordinary circumstances lead to a serious threat to public security or public health in the EU.[124]

Secondly, VLOPs are subject to yearly independent audits in order to assess compliance with the obligations and responsibilities set out in the DSA.[125] Additionally, they must provide the relevant authorities with access to data and information that are necessary to monitor and assess compliance with the DSA.[126] In order to monitor compliance internally, VLOPs must also establish a compliance function that is independent from the operational functions.[127]

Finally, there are also additional obligations regarding recommender systems and a higher standard of online advertising transparency for VLOPs.[128] The reporting obligations applicable to VLOPs also require a higher standard of transparency as compared to intermediary services that do not qualify as VLOPs.[129]

2.5.4 What is important for KRAKEN?

As an online marketplace for personal data, which constitutes a digital service, the DSA is potentially relevant for the KRAKEN platform. Considering the scope of application and accompanying categorization of intermediary services, the KRAKEN platform does not qualify as a mere conduit or cashing service, but rather as a *hosting service*. This is the case even though the KRAKEN platform does not directly store any data products, as it facilitates the coming together of data providers and data consumers as well as the transaction and transfer of data products between them. Similar to other online marketplaces that do not directly store products, the KRAKEN platform allows its users to publish information on data products in order to connect with potential data consumers. Moreover,

[120] Ibid., Art. 24d (3).
[121] Ibid., Art. 24e (1).
[122] Ibid., Recital 54 and Art. 25.
[123] Ibid., Art. 26 and 27.
[124] Ibid., Art. 27a.
[125] Ibid., Art. 28.
[126] Ibid., Art. 31.
[127] Ibid., Art. 32.
[128] Ibid., Art. 29 and 30.
[129] Ibid., Art. 33.

the KRAKEN platform qualifies as an *online platform*. Considering that, as an online marketplace, the KRAKEN platform disseminates information to the public at the request of a recipient, which is a principal feature of the platform, it satisfies the definition of an online platform. This reasoning is not only in line with the spirit of the DSA, but is also confirmed by EU institutions in their statement that online marketplaces qualify as online platforms and by extension as hosting services.[130] Consequently, the KRAKEN platform will have to respect the layered obligations as laid down in the DSA.

It is important to note that the KRAKEN platform would benefit from the liability exemption for hosting services laid down in Article 5 of the DSA proposal. As a result, the KRAKEN platform would not be liable for the information stored at the request of a recipient on the condition that the KRAKEN platform (a) does not have actual knowledge of illegal activity or illegal content and is not aware of facts or circumstances from which the illegal activity or illegal content is apparent; or (b) upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the illegal content. Actual knowledge or awareness could be obtained through a notice from a third party or by conducting voluntary own-initiative investigations, which would result in the KRAKEN platform having to take action against the illegal content.[131] Moreover, the KRAKEN platform cannot be obliged to generally monitor the information which it transmits or stores, nor to actively seek facts or circumstances indicating illegal activity.[132] Conducting voluntary own-initiative investigations and taking measures in good faith and in a diligent manner does not make KRAKEN ineligible for the liability exemption mentioned in this paragraph.[133] It must also be reiterated that the KRAKEN platform does not store any data products (i.e., batch data) of recipients, but rather stores information about that data product provided by those recipients. Consequently, the KRAKEN platform is not able to remove or disable access to the alleged illegal content itself, but rather to the information about that alleged illegal content.

Following the layered approach, as (1) an intermediary service, (2) a hosting service, and (3) an online platform, the KRAKEN platform would fall under three cumulative layers of obligations. The fourth layer, which applies to VLOPs, does not apply to the KRAKEN platform due to the threshold of 45 million average monthly recipients in the EU. Moreover, the DSA also acknowledges that some of the abovementioned obligations are too burdensome for micro and small enterprises. Depending on the final adoption and exploitation, if the KRAKEN platform meets the threshold for the qualification as a micro or small enterprise, the obligation applicable to intermediary service providers to publish an annual report on content moderation activities as well as all obligations applicable to online platforms, except Article 23 (3), would not apply.

2.6 The Data Markets Act

2.6.1 What is it and what does it aim for?

The Council has adopted the DMA on 18 July 2022. It will become directly applicable in the EU six months after its entry into force, which occurs twenty days after its publication in the Official Journal of the European Union.[134] The DMA establishes a harmonized framework to level the playing field for

[130] Ibid., Recital 13; European Commission, Digital Services Act: Commission welcomes political agreement on rules ensuring a safe and accountable online environment, https://ec.europa.eu/commission/presscorner/detail/en/IP_22_2545; and European Parliament, Briefing: EU Legislation in Progress: Digital services act, https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689357/EPRS_BRI(2021)689357_EN.pdf, 4.

[131] Recital 22 and Art. 6 DSA Proposal.

[132] Ibid., Art. 7.

[133] Ibid., Art. 6.

[134] Art. 54 of Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828

digital companies, regardless of their size. It establishes clear rules for big platforms and aims to guarantee a competitive and fair digital sector by giving the possibility for business users to offer more choices to consumers, banning unfair practices of large online platforms, imposing clear rights and obligations on large online platforms, promoting innovation and a fairer online environment for start-ups, and more.[135]

2.6.2 Scope of application

The DMA applies to *core platform services* provided or offered by *gatekeepers* to business users[136] established in the EU or end users[137] established or located in the EU, irrespective of the place of establishment or residence of the gatekeepers.[138] The DMA also provides a list of core platform services that fall under its scope:

- online intermediation services (i.e., marketplaces, app stores, etc.);
- online search engines;
- online social networking services;
- video-sharing platform services;
- number-independent interpersonal communications services;
- operating systems;
- web browsers;
- virtual assistants;
- cloud computing services; and
- online advertising services.[139]

Chapter II of the DMA establishes that an undertaking qualifies as a gatekeeper if: (1) it has a significant impact on the internal market, (2) it provides a core platform service which is an important gateway for business users to reach end users, and (3) it enjoys an entrenched and durable position, in its operations, or it is foreseeable that it will enjoy such a position in the near future.[140] In order to satisfy the first requirement, an undertaking must achieve an annual turnover of EUR 7,5 billion or more in each of the last three financial years or have an average market capitalization or an equivalent fair market value of at least EUR 75 billion in the last financial year. It must also provide the same core platform service in at least three Member States.[141] For the second requirement, an undertaking must provide a core platform service that in the last financial year has at least 45 million monthly active end users established or located in the EU and at least 10 000 yearly active business users established in the EU.[142] For the third and final requirement, an undertaking must have met the thresholds of the

(Digital Markets Act) (hereafter 'the DMA'); European Commission, The Digital Services Act package, https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package; and European Council and Council of the European Union, Digital services package, https://www.consilium.europa.eu/en/policies/digital-services-package/.

[135] Art. 1 DMA; and European Council and Council of the European Union, Digital services package, https://www.consilium.europa.eu/en/policies/digital-services-package/.

[136] Art. 2 (21) DMA defines business user as "*any natural or legal person acting in a commercial or professional capacity using core platform services for the purpose of or in the course of providing goods or services to end users*".

[137] Art. 2 (20) DMA defines end user as "*any natural or legal person using core platform services other than as a business user*".

[138] Ibid., Art. 1 (1).

[139] Ibid., Art. 2 (2); and European Council and Council of the European Union, Digital services package, https://www.consilium.europa.eu/en/policies/digital-services-package/.

[140] Ibid., Art. 3 (1).

[141] Ibid., Art. 3 (2) (a).

[142] Ibid., Art. 3 (2) (b).

second requirement in each of the last three financial years.[143] These three cumulative requirements set a very high threshold for undertaking to qualify as gatekeepers.

2.6.3 Obligations for gatekeepers

This section will briefly describe some of the positive and negative obligations imposed on gatekeepers. Considering the high threshold for qualification as a gatekeeper and the limited relevance for the KRAKEN platform, these obligations will not be described in detail.

Under the DMA, gatekeepers are obliged to:

- offer more choices (e.g., software on a user's operating system)[144];
- ensure that unsubscribing from core platform services is as easy as subscribing[145];
- provide information on the number of users that visit their platforms[146];
- give business users access to marketing or advertising performance data on the platform[147];
- inform the European Commission on acquisitions and mergers[148]; and
- ensure that basic functionalities of instant messaging services are interoperable.[149]

On the other hand, gatekeepers are not allowed to:

- rank their own products or services higher than those of others[150];
- prevent developers from using third-party payment platforms for app sales[151];
- process, combine, and cross-use the users' personal data in specific ways for targeted advertising, unless consent has been obtained[152];
- establish unfair conditions for business users[153];
- pre-install specific software applications or prevent users from easily uninstalling them[154]; and
- restrict business users of the platform[155].

2.6.4 What is important for KRAKEN?

As an online intermediation service (i.e., an online marketplace), the subject matter of the DMA is relevant for the KRAKEN platform. However, considering the strict requirements and high thresholds for qualification as a gatekeeper, is seems highly unlikely that the KRAKEN platform would fall under the scope of the DMA. Depending on the final adoption and exploitation of the KRAKEN platform, although unlikely, it remains to be seen whether or not the obligations imposed on gatekeepers will be applicable to KRAKEN.

[143] Ibid., Art. 3 (2) (c).
[144] Ibid., Art. 6 (4).
[145] Ibid., Art. 6 (13).
[146] Ibid., Art. 14 (2).
[147] Ibid., Art. 6 (8).
[148] Ibid., Art. 14.
[149] Ibid., Art. 7 (1) and (2).
[150] Ibid., Art. 6 (5).
[151] Ibid., Art. 5 (7).
[152] Ibid., Art. 5 (2).
[153] Ibid., Art. 6 (12).
[154] Ibid., Art. 6 (3).
[155] Ibid., Art. 5 (4) and (6).

3 Ethical and legal evaluation of KRAKEN

Deliverable 7.2 provided a broad array of legal requirements. Not all requirements are technical (T), many are organizational (O) and can only be fulfilled when KRAKEN would be employed as a service by a legal entity. Therefore, the analysis focuses on those requirements that can be fulfilled on a technical level and whether these have been taken into account in the development of the KRAKEN system.

During the development of the KRAKEN system, two reviews were conducted, and feedback provided on the user interface, respectively on the 31.5.2021 and on 1.3.2022.

For the applicability of the requirements, and in how far they must be fulfilled, the role of the controller is important. For the KRAKEN system, as explained in D7.2, different constellations are possible. However, certain requirements are applicable to KRAKEN directly as a controller in the context of account data, while other requirements are more applicable in the function of the KRAKEN system as supporting controllers with the exchange of data in a compliant way.

3.1 Analysis KRAKEN as a controller for account data

KRAKEN acts as the sole controller for the processing of account data by determining the means and purposes of processing. Consequently, KRAKEN is responsible for satisfying the data protection obligations laid down by the GDPR. In addition to the current analysis, tables with the evaluation and validation of ethical and legal requirements (Table 1. Requirements for KRAKEN as a controller of account data, Table 2: Requirements for KRAKEN as data exchange service provider, Table 3: Requirements for KRAKEN as data analytics provider. Table 4: Requirements for KRAKEN as a provider of an information society service) can also be found in the Annex

Analysis implementation requirements:

DP-1 (O/T): Identify the type of data which will be processed

Different data protection obligations may apply depending on the specific type of data being processed. Following the risk-based approach of the GDPR, the processing of personal data that involves a higher risk for the rights and freedoms of natural persons also incurs more stringent obligations and a higher standard of protection.

In KRAKEN, account data is requested and collected when creating a KRAKEN user account, which includes the following: first name, last name, e-mail address, country of residence, and 18 years or older. Account data is limited to these types of data, which are also listed in the KRAKEN Privacy Policy, and do not include special categories of personal data.

DP-2 (O): Define roles: identify who acts as controller and who acts as processor

KRAKEN acts as the sole controller in relation to account data by determining the means and purposes of processing. The relevant information on the different roles is also included in the KRAKEN Privacy Policy.

DP-2.1 (O): IF controller-processor relationship: establish controller-processor agreement in writing

This requirement is not applicable. There are no other parties that act as processors in relation to account data.

DP-2.2 (O): IF joint controller relationship: establish joint controller agreement and make the essence of the arrangement available to the data subject

This requirement is not applicable. KRAKEN is the sole controller in relation to account data.

DP-2.2.1 (O): The joint controller agreements should include the allocation of respective responsibilities for compliance with the obligations under this Regulation

By extension, this requirement is also not applicable.

DP-3 (O): Identify the purposes of the data processing

For the processing of account data, two separate purposes can be identified.

Firstly, the processing of account data is necessary to create and maintain a KRAKEN user account and make use of the KRAKEN platform service, which means to publish and make available a data product or obtain access to a data product on the KRAKEN platform.

Secondly, the processing of account data may also be necessary in order to comply with a legal obligation for the purpose of legal compliance, tax or auditing purposes, or to detect and prevent fraudulent or illegal activity.

DP-3.1 (O): IF data is processed for another purpose AND not based on consent or legislation: controller must make an assessment on whether the processing is compatible with the purpose for which the personal data are initially collected

This requirement is not applicable. KRAKEN does not process account data for purposes other than the original purposes listed in the Privacy Policy. In case additional purposes are identified in the future, KRAKEN should update the relevant information included in the Privacy Policy, and where necessary, make an assessment on the compatibility of purposes.

DP-4 (O): Identify the legal ground of processing

KRAKEN processes account data based on the necessity for the performance of a contract between KRAKEN and the user, which exists in the creation and maintenance of a KRAKEN user account and the subsequent usage of the KRAKEN platform service.

It may also be the case that KRAKEN processes account data based on a legal obligation for the purpose of legal compliance, tax or auditing purposes, or to detect and prevent fraudulent or illegal activity.

DP-4.1 (O/T): IF the processing is based on consent: the controller must be able to demonstrate that the data subject has consented to processing of his or her personal data

This requirement is not applicable. The processing of account data is not based on the consent of the data subject.

DP-4.1.1 (O/T): Consent must comply with the requirements of the GDPR

By extension, this requirement is not applicable.

DP-4.1.2 (O/T): Include the possibility to check that the person consenting is 18 years or older

This is not a requirement laid down by the GDPR. Member States may decide on the age of consent, which therefore varies between Member States. Parents can also give consent to the processing of their children's data. For general use a minimum age of 18 is the simplest solution, also from an ethical point of view in order to provide that the data subject has a certain autonomy in their decision-making.

Although the processing of account data is not based on the consent of the data subject, users must state that they are 18 years or older in order to create a KRAKEN user account.

DP-4.2 (O): IF the processing is based on the ground that it is necessary for the purposes of the legitimate interests pursued by the controller or by a third party: it must be ensured that the interests are not overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child

This requirement is not applicable. The processing of account data is not based on the legitimate interests of the controller.

DP-4.3 (O/T): IF special categories of personal data are processed: explicit consent needed

This requirement is not applicable. Account data does not include special categories of personal data.

DP-4.4 (O): IF the processing is based upon the necessity for the performance of a contract: only process the data relevant for the contract

The processing of account data is limited to personal data that is strictly necessary for the performance of the contract between KRAKEN and the user, which exists in the creation and maintenance of a KRAKEN user account and the subsequent usage of the KRAKEN platform service.

Specific data such as the country of residence and 18 years or older is required to observe specific national obligations and requirements, such as national data protection provisions.

DP-5 (O/T): Keep written records of processing activities

The processing of account data by KRAKEN is limited in scope and the information on the processing activities related to account data are included in the KRAKEN Privacy Policy.

The SSI and registration modules provide correspondent log files. Marketplace registration events are logged in the marketplace Backend database.

DP-5.1 (O): Be able to make the written records available to the supervisory authority on request

Information on the processing activities related to account data are included in the KRAKEN Privacy Policy. The log files related to SSI and user registration, product publication or product consumption within the marketplace can be made accessible to the supervisory authority.

DP-6 (O/T): Facilitate the exercise of data subject rights

Data subjects may contact KRAKEN to exercise their rights as a data subject in relation to account data. Information on how to exercise data subject rights and relevant contact details may be found in the KRAKEN Privacy Policy.

According to article 23 of the GDPR, national legislation may impose additional restrictions on the exercise of data subject rights.

DP-6.1 (O/T): Establish measures to easily retrieve information in case an access request or an audit is filed

KRAKEN is able to respond to access requests and provide the data subject with the necessary and relevant information. Relevant information may also be found in the KRAKEN Privacy Policy.

DP-6.2 (O/T): Be able to stop the processing of personal data when a data subject request requires it

By contacting KRAKEN, data subjects are able to object at any time to the processing of their account data for direct marketing purposes, which includes profiling to the extent that it is related to such direct marketing.

Data subjects may also indirectly object to the processing of their account data by exercising their right to erasure (by deleting their KRAKEN user account through the KRAKEN user profile or by contacting KRAKEN).

DP-6.3 (O/T): Be able to rectify the data without undue delay

Data subjects are able to rectify their account data through the KRAKEN user profile or by contacting KRAKEN.

DP-6.4 (O/T): Be able to communicate any rectification, erasure or restriction of processing to each recipient to whom the personal data have been disclosed

Account data will never be transferred or made accessible to third parties, unless such a transfer is necessary to comply with a legal obligation, in which case KRAKEN should communicate any rectification, erasure or restriction to those recipients.

DP-6.5 (O/T): Be able to erase the data without undue delay

Data subjects are able to obtain the erasure of their account data by deleting their KRAKEN user account through the KRAKEN user profile or by contacting KRAKEN.

As the information is kept on the Marketplace Registration Verifiable Credential (VC) which is under control of the user, the user can decide themselves how long the data should be made available. No personal data of the user is stored on the blockchain.

DP-6.5.1 (O/T): IF the data was made public and must be erased due to a data subject request: take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data

Account data will never be transferred or made accessible to third parties, unless such a transfer is necessary to comply with a legal obligation. In any case, account data will never be made publicly available.

DP-6.6 (O/T): If automated individual decision-making is used: make sure the data subject is aware of it, has a possibility to object against it and provide the possibility to include a 'human in the loop'

This requirement is not applicable. Automated individual decision-making is not used in relation to account data.

DP-7 (O): Implement a data protection policy

For account data, KRAKEN implements a data protection policy through the KRAKEN Privacy Policy.

DP-8 (O): Provide information to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language and in writing

The KRAKEN Privacy Policy contains information relating to processing of account data in a concise, transparent, intelligible and easily accessible form, using clear and plain language. For additional information and questions regarding the processing of account data, data subjects may contact KRAKEN.

DP-9 (O/T): Data Protection by design: Implement appropriate technical and organizational measures which are designed to implement data-protection principles in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects

KRAKEN implements technical and organizational measures to adhere to the requirements of the GDPR and to protect the rights of data subjects. Examples of measures are strong web security, end-to-end encryption, access & storage policies, and functionalities to easily exercise data subject rights.

DP-10 (O/T): Data Protection by default: Implement appropriate technical and organizational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed

KRAKEN, by default, only collects and processes account data that are strictly necessary for the listed purposes. The extent and period of processing of account data are also limited to what is strictly necessary for those purposes.

DP-11 (O): In case of personal data breach which might result in a risk to the rights and freedoms of natural persons: notify without undue delay and if possible, no later than 72 hours after becoming aware of it to the competent supervisory authority

In case of a data breach, KRAKEN should contact the supervisory authority to provide relevant and necessary information in accordance with article 33 GDPR.

DP-11.1 (O): Document any personal data breach: the facts relating to the breach, its effects and the remedial actions taken

In case of a data breach, KRAKEN should document the breach in accordance with article 33 (5) GDPR.

DP-11.2 (O): In case of a personal data breach which might result in a high risk to the rights and freedoms of natural persons, communicate the breach in clear and plain language and without undue delay to the data subject

Although a high risk to the rights and freedoms of natural persons is unlikely considering the types and non-sensitive nature of the account data in question, in such a case KRAKEN should communicate the breach to the data subject in accordance with article 34 GDPR.

DP-12 (O): In case the processing is likely to result in a high risk to the rights and freedoms of natural persons: make a DPIA before the processing.

This requirement is not applicable. The processing of account data by KRAKEN is not likely to result in a high risk to the rights and freedoms of natural persons considering the types, non-sensitive nature, and extent of processing activities.

DP-13 (O): IF engaging a processor: only use processor providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject

This requirement is not applicable. KRAKEN is the sole controller in relation to account data. There are no other parties that act as processors in relation to account data.

DP-14 (O/T): Establish technical and organizational security measures to deploy in the processing and storage of information

The processing of account data is not likely to incur a high risk to the rights and freedoms of natural persons. Although this risk is low considering the types and non-sensitive nature of the account data in question, it is still important to implement appropriate technical and organizational security measures.

DP-14.1 (O/T): Should implement pseudonymization and encryption of personal data

KRAKEN implements end-to-end encryption to protect the confidentiality of data in transit.

DP-14.2 (O/T): Should be able to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services

Measures such as strong web security, end-to-end encryption, and access & storage policies aim to protect confidentiality, integrity, availability, and resilience of systems and services.

DP 14.3 (O/T): Should be able to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

In case of an incident, KRAKEN can restore the availability of account data, which has a cloud backup, in a timely manner.

Account data is also stored on the Marketplace Registration VC which is in control of the KRAKEN user.

DP-14.4 (O/T): Should have a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing

Technical and organizational security measures should be periodically tested and reviewed by KRAKEN.

DP 14.5 (O/T): Should take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law

By implementing access policies and providing clear instructions, KRAKEN aims to limit processing of account data to what is necessary and instructed.

DP-15 (O): If necessary, designate a data protection officer and publish the contact details of the DPO and communicate them to the supervisory authority

This requirement is not relevant for the processing of account data. However, in relation to content data, due to the potentially high volume of personal data, including special categories of personal data, the KRAKEN platform should designate a data protection officer (DPO) and make their contact details available to the public and supervisor authority.

DP-16 (O/T): Only transfer personal data to a third country or an international organization if one of the conditions is given and therefore the level of protection guaranteed by the GDPR is not undermined

This requirement is not applicable. KRAKEN does not transfer account data to third countries or international organizations.

3.2 Analysis KRAKEN as a data exchange service

In this role, KRAKEN itself does not have the role of a controller or processor, as it does not process the data, nor decide on the purposes and means of processing, but rather provides a service to bring data provider and data consumer in contact with each other. The controller has the final responsibility to choose the correct service and comply with the data protection obligations. Nevertheless, the KRAKEN service should simplify this compliance for the controller. Two controllers might be included in a data transfer, on the provider side it is possible that the provider will be a controller, and on the receiver side the receiver will always be a controller. The providing controller has to ensure that it is legally allowed to provide access to the data and that all obligations, including information obligations have been complied with. This is, however, outside of the scope of the KRAKEN system, and the only possibility for KRAKEN is to provide an indication that the providing controller must confirm to have complied with all obligations and is allowed to give access to the data. The receiving controller must comply with the data protection obligations, when the data has been provided by a providing controller, but also when the data is provided directly by a data subject. KRAKEN can support the compliance by e.g., establishing which information the receiving controller needs to provide, providing the possibility to obtain consent and giving the possibility to keep recordings of the received consent. Below a selection of the analysis will be provided, since there are certain requirements, in particular those which are entirely organizational, which KRAKEN as a service provider not involved in the processing cannot fulfill. The full analysis can be found in the Annex in Table 2: Requirements for KRAKEN as data exchange service provider

Analysis implementation requirements:

DP-1: Identify the type of data which will be processed

When publishing data, the provider has to indicate whether or not the data they provide includes personal data, since the provider might also provide anonymous data. In a second step, the data provider indicates whether or not the personal data includes sensitive personal data (special categories of personal data). In principle this requirement is fulfilled, though it might be useful to add some information on what exactly the meaning of personal data and sensitive personal data is, so that a data provider who does not know the terms can still make the correct choice.

DP-2: Identify who is controller and who processor

For the receiving controller, when buying access to the data, the screen shows an information that specifies that "by receiving and processing personal data you are considered a data controller under the General Data Protection Regulation and are consequently subject to its obligations. In particular, this includes that data subjects have the right to request from you the exercise of the data subject rights provided by the General data Protection Regulation, which includes: access to and rectification or erasure of their personal data, the restriction of or objection to the processing of their personal data, as well as the right to data portability. Data subjects also have the right to withdraw their consent at any time. For more information on the rights of the data subjects please consult KRAKEN's privacy policy".

Regarding the sign up and provision of the data, no differentiation between the roles of providing controller and data subject has been implemented (though it has been recommended). A clear separation would make it easier for the data provider to understand which role and obligations they have, and to provide the necessary information to the data subject.

DP-3: Identify the purpose of the data processing

When providing the data and when buying access to the data, the user interface requires to select purposes, and allows only access to the data when the purposes match. The selection of purposes is at the moment: Marketing, management or improvement of business services, publicly funded research, private research and automated decision-making, e.g., Artificial intelligence (including profiling). In principle, this requirement can be fulfilled with this, however, as the purposes are supposed to be specific, it would be better to add more possibilities for selection or a blank field.

DP-4: Identify the legal ground for processing

The legal ground for processing in the case of batch data and data analytics is consent. Accordingly, the following sub-requirements apply:

DP-4.1 (O/T): Consent: IF the processing is based on consent: the controller must be able to demonstrate that the data subject has consented to processing of his or her personal data

Access to the data is only provided if the parameters given by the data provider match the parameters provided by the data consumer. The parameters entailing the consent of the data subject are stored on the Lynkeus blockchain, and therefore, it is possible to demonstrate that the data subject consented to the processing of his or her personal data.

DP-4.1.1 (O/T): Consent must comply with the requirements of the GDPR

The consent must be an indication of the data subject's wishes which signifies agreement to the processing of his/her personal data. In the case of the provision of data via KRAKEN, this should normally apply, as the data subject actively provides the data, specifying the exact terms under which it will provide the data. The consent must be freely given, which again, should be fulfilled as it is a free choice of the data subject to provide the data. The possibility exists that outside of the KRAKEN system users are coerced into providing the data, however, this is outside of the possibility for the KRAKEN system to detect. In such a case the consent will not be valid.

The consent must also be specific and informed. In principle, this is fulfilled as the data subject can indicate who can receive which data, for how long and for which purposes. However, at the moment the selection of purposes is rather restricted, accordingly it would be better if, when the system would be further improved, to expand the potential purposes and/or add a free field.

An open question is whether the data subject can be considered informed, if it does not know who will be processing his/her data at the moment of giving the consent. However, considering that the data subject is able to select who is allowed to process the data, and will get the required information in the dashboard as soon as the data consumer obtained access to the data, it is assumed that the data subject is sufficiently informed.

As it is the own action of the data subject which provides the access to the data, while clearly knowing and indicating for what the data may be used, the consent is considered to be unambiguous.

There must be a possibility to withdraw consent at any time, and it must be as easy to withdraw as to give consent. In the KRAKEN system this is possible via the marketplace mobile app, where the data subject has an overview of who has currently access to the data and an easy possibility to withdraw the consent.

Before giving consent, the data subject must be informed that a withdrawal shall not affect the lawfulness of processing based on consent before its withdrawal.

DP-4.1.2: Include possibility to check that the person consenting is over 18

At sign up, the person signing up has to confirm that they are over 18.

DP-4.3: IF special categories of personal data are processed: explicit consent needed

Though it would only be necessary when the data provider indicates that the data includes special categories of data, nevertheless, the consent is done in such a way, and by concluding several independent steps, that normally the requirements for explicit consent are always fulfilled.

DP-6: Facilitate the exercise of data subject rights

As the KRAKEN system does only facilitate the exchange but is not involved in the actual processing, the exercise of data subject rights depends on the receiving controller, who must be able to comply with the obligations. The KRAKEN system can facilitate the exercise of data subject rights, by giving the data subject an easy way to exercise their data subject rights towards the receiving controller via the dashboard.

Potential improvements in this regard could be to simplify the exercise of data subject rights even more by providing e.g., a menu for the data subject to exercise their data subject right. For example, a simple way to indicate that they wish to have the data rectified or erased. In principle, the data subject should be able to do this directly in their own data, however, the problem exists that the receiving controller downloaded the data and has the erroneous or not wished for data now stored in their own system.

DP-6.6 (O/T): **If automated individual decision-making is used:**

In case automated decision making is used, it must be possible to make sure the data subject is aware of it, provide a possibility to object against it and provide the possibility to include a ‘human in the loop’.

The data provider is aware of the processing, as he can select whether he agrees with the use of the data for automated decision making and can simply object against it by not making it available for this purpose.

When the data provider indicates the agreement with the automated decision-making purpose, he also needs to indicate which workings and potential significance and envisaged consequences of automated decision making are approved: automated placing of services and product offerings, hiring assessments, clinical risks assessment, diagnostic or treatment suggestions.

The possibility to include a 'human in the loop' is a requirement that needs to be fulfilled at the receiving controller's side.

DP-8 (O/T): Information: Provide information to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language and in writing

It is aimed for to provide the information to the data subject in a clear and easily accessible form. With a split in data provision between data subject and providing controller, this would be easier. More detailed information can be provided, but this was not in the scope of the current work for the UI.

DP-9 (O/T): Data protection by design: Implement appropriate technical and organizational measures which are designed to implement data-protection principles in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects

The KRAKEN system gives the data subject the possibility to indicate which data under which circumstances might be processed by which entity. Furthermore, it gives the possibility to encrypt the batch data in order to keep it secure and avoid access from data consumers which do not fulfill the requirements set out by the data subject.

DP-10 (O/T): Data protection by default: **Implement appropriate technical and organizational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed**

It is not possible for KRAKEN to verify whether the provided personal data is indeed necessary for the indicated purpose. It is expected that the data subject and data consumer only indicate to share data, which is necessary for the indicated purpose, whereby it would be recommended to extend the selection of purposes.

DP-14 (O/T): Security: **Establish technical and organizational security measures to deploy in the processing and storage of information**

KRAKEN provides encryption of the batch data and does not keep the data at its system. The product publication and product consumption processes can only be completed if the data product has been encrypted and decrypted in the marketplace Frontend. Accordingly, the security requirements are not for the KRAKEN system but for the receiving controller.

DP-16 (O/T): Third country Data Transfer

This requirement provides that personal data may only be transferred to a third country or an international organization if one of the conditions is given and therefore the level of protection guaranteed by the GDPR is not undermined:

- transfer is on the basis of an adequacy decision;
- transfer is subject to appropriate safeguards;
- transfer is based on biding corporate rules; or
- one of the derogations of art. 49 is applicable.

In the KRAKEN system, the data provider can indicate to which countries the data may be transferred. This is done by indicating at the question to which country and region may the data be transferred, whether they allow a transfer to EU/European Economic Area (EEA) countries, non-EU/EEA country with an adequacy decision, or non-EU/EEA country without an adequacy decision. In the last case, a warning applies that if this option is chosen, there will be no safeguards from the GDPR applying to the processing. However, in order to still keep the level of protection guaranteed by the GDPR, the agreement between the data provider contractually obliges the data consumer to comply with the GDPR.

A potential problem with that solution is, however, that the data subject might not be able to sue the receiving controller in case of a breach of contract. Accordingly, it might be worth considering not to include non-EU/EEA countries without an adequacy decision, except if it could be validated in some way that they provide an equivalent level of protection to the GDPR.

3.3 Analysis KRAKEN as an analytics provider

The KRAKEN system provides the option for data analytics. The data provider can indicate that the provided data might be also or exclusively used for data analytics. For that, the data is split into shares and the data provider uploads them in an encrypted form that can be accessed only by the secure multi-party computation (SMPC) nodes (servers participating in the SMPC network).[156] Without knowing enough of the shares, no information about the data can be revealed. The shares are distributed among SMPC nodes, so that they can interactively compute a function on the data without knowing the data or the result themselves. The (shares of) results are delivered to a buyer of a computation, who can merge them in the final result.

Analysis implementation requirements:

DP-1 (O/T): Types of data: Identify the type of data which will be processed

Depending on the type of data, different obligations are applicable.

When publishing data, the provider has to indicate whether or not the data they provide includes personal data, and in a second step, whether or not the personal data includes sensitive personal data. In principle this requirement is fulfilled, though it might be useful to add some information on what exactly the meaning of personal data and sensitive personal data is, so that a data provider who does not know the terms can still make the right choice.

Furthermore, it has been stated by the developers that the output of the SMPC analysis will not constitute personal data. In that case, the GDPR requirements will not be applicable to the output. However, it would need to be verified whether this is indeed in all circumstances the case.

DP-2 (O): Define roles: Identify who is controller and who processor

Who the controller and processor will be depends upon the factual situation and can accordingly change depending on the circumstances. As will be explained further below in the section 6.2, considering the European Court of Justice (ECJ) case law on joint controllership, a possibility exists that the KRAKEN platform could be considered a joint controller. However, since the whole process of analytics is not done in the own interest of KRAKEN, but as a service for the data provider and data consumer, we assume here that KRAKEN will be acting as a processor. The SMPC nodes will normally be external to the KRAKEN platform, and can be considered as sub-processors. In case the relative approach to anonymization is followed (see section The anonymization of personal data for more information), it might also be possible to argue that, since the shares do not reveal information by themselves, the SMPC nodes will not be processing personal data. Assuming that the result of the analytics will be anonymous as claimed by the KRAKEN developers, the only processing of personal data would then be the splitting and encrypting of the personal data into shares.

DP-2.1 (O): IF controller-processor relationship: establish controller-processor agreement in writing

As a purely organizational requirement, this requirement is at the moment not implemented.

Obligations processor:

DP-14 (O/T): Security: **Establish technical and organizational security measures to deploy in the processing and storage of information**

[156] KRAKEN D5.4 ‘Final KRAKEN marketplace integrated architecture’, 18.

DP-14.1 (O/T): Should implement pseudonymization and encryption of personal data

Since the processing that KRAKEN provides is actually the splitting of the personal data into shares, encrypting, and analysing them, after which they are given to the data consumer, this requirement is fulfilled.

DP-14.2 (O/T): Should be able to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services

As the key shares are shared to the SMPC nodes, and each SMPC node only receives a part of the data, the confidentiality is ensured. Integrity, availability and resilience are the responsibility of the data provider, as KRAKEN has not access to the full dataset.

DP-14.3 (O/T): Should be able to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

As KRAKEN sends the encrypted data to the data consumer, it is not possible to restore the availability or access to personal data afterwards, as it is not located at the KRAKEN platform anymore and becomes the responsibility of the data consumer after it has been given back to them.

DP-14.4 (O/T): Should have a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

The system has been tested during development, however, when the system is implemented a process for regularly testing, assessing and evaluating the measures would need to be established. This to make sure that the encryption is functioning, and personal data will not become available to anybody except the encryption service for the purpose of encrypting the data.

DP-14.5 (O/T): Should take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law

As the encryption, though provided by KRAKEN, takes place at the side of the data provider, normally no natural person working for KRAKEN would have access to the data.

DP-15 (O): DPO: If necessary, designate a data protection officer and publish the contact details of the DPO and communicate them to the supervisory authority

As an organizational requirement, this is currently not applicable and will only be necessary to be fulfilled when the KRAKEN platform acts in the market.

DP-16 (O/T): Third country Data Transfer

Only transfer personal data to a third country or an international organization if one of the conditions is given and therefore the level of protection guaranteed by the GDPR is not undermined:

- transfer is on the basis of an adequacy decision;
- transfer is subject to appropriate safeguards;
- transfer is based on biding corporate rules; or
- one of the derogations of art. 49 is applicable.

As the SMPCs and the KRAKEN platform are all located within the European Union, and the result of the analysis is considered to be anonymous, this requirement is not applicable.

DP-17 (O/T): Provide sufficient guarantees to implement appropriate technical and organizational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.

The only processing in this scope is the encryption of the data for the SMPC analytics. When complying with the requirements set out here, it will be assumed that this requirement will be fulfilled.

DP-18 (O): Don't engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.

As an organizational requirement this is not applicable at the moment, however, whether it will be relevant in the exploitation of KRAKEN will depend on whether the SMPCs will be considered as sub-processors or not.

DP-19 (O): IF the processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor shall be imposed on that other processor by way of a contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of this Regulation.

As an organizational requirement, it is not applicable at the moment.

DP-20 (O): Only process data upon instructions of the controller (except required to do so by Union or Member State law)

As an organizational requirement, it is not applicable at the moment.

DP-21 (O/T): Keep a written record of all categories of processing activities

The only processing activity taking place is the encryption of the data, which is not an ongoing processing activity, but only an incidental one, and the data is not kept by the KRAKEN platform.

DP-22 (O): Notify controller in case of a data breach

As an organizational requirement, it is not applicable at the moment.

3.4 Analysis KRAKEN as a provider of an information society service

As detailed in Chapter VI of D7.3 'Ethical and legal requirement specification', the KRAKEN service can be considered as an information society service. Consequently, the provisions of the e-Commerce Directive are relevant for the KRAKEN platform. In order to satisfy the different requirements and conditions resulting from the various national implementations of the Directive, it is necessary to consider the Member State where the KRAKEN platform provider will be established in the future.

It is important to note that the e-Commerce Directive will be partially amended by the upcoming DSA. The e-Commerce Directive lays down harmonized rules on the conditional exemption from liability for providers of intermediary services, which are reiterated and clarified in the upcoming DSA.[157]

Chapter VI of 'Ethical and legal requirement specification' also mentions the Platform-to-Business Regulation, which aims at promoting fairness and transparency for business users of online intermediation services. By taking into account the definition of an online intermediation service, KRAKEN would also fall under the scope of this Regulation. It is likely that data providers can be

[157] Recital 16 DSA Proposal.

considered as business users[158], but less likely that data receivers can be considered as consumers[159]. Since this scenario is not wholly excluded, the Regulation has been included in the analysis.

Analysis implementation requirements:

ECOM-1: Establish whether the user is acting as a consumer or a business user

The current KRAKEN user interface (UI) does not include the possibility for a user to signify whether they are acting as a business user or as a consumer for a given transaction. Even though this requirement has not been fulfilled at this point in time, it is still possible to satisfy the other requirements that result from the qualification as a business user or as a consumer (e.g., terms and conditions in plain and intelligible language, easily available, etc.).

ECOM-2: Include easily reachable information on the service provider

The service provider should render easily, directly and permanently accessible to the recipients of the service and competent authorities, at least the following information: the name of the service providers, the geographic address at which the service provider is established, details of the service provider (incl. e-mail address), the trade register and registration number in case of registration in a trade or similar public register, and the tax identification number in case of an activity that is subject to VAT.[160]

This requirement is dependent on the final adoption and exploitation of the KRAKEN platform, particularly on the identity and establishment of the entity that will provide the KRAKEN platform service. Consequently, this requirement should be implemented at the time such information is available.

ECOM-3: Provide information for the conclusion of a contract with a consumer

The service provider should provide the following information in a clear, comprehensible, and unambiguous manner prior to the order being placed by the recipient: the different technical steps to follow to conclude a contract, whether or not the concluded contract will be filed by the service provider and whether it will be accessible, the technical means for identifying and correcting input errors prior to the placing of the order, and the languages offered for the conclusion of the contract. Parties who are not consumers (i.e., business users) may agree to relinquish this requirement.[161]

The KRAKEN UI guides the user through the different steps in order to publish or obtain access to a data product. Prior to placing the order, the user is able to identify and correct any input errors by assessing the final overview page of the order. The contract between KRAKEN and the user is concluded by publishing or obtaining access to a data product and accepting the Terms and conditions of the KRAKEN platform. Furthermore, an agreement is closed between the data providers and data consumers which involves accepting the agreement between data providers and data consumers (which is currently at the sign-up page, but should be moved to the data provision/acquiring page). It should be noted that contractual law is national, which has implications on the conclusion of the agreements and should be taken into account for the final implementation and exploitation of the platform.

[158] Art. 2 (1) of the Platform-to-Business Regulation defines business user as "*any private individual acting in a commercial or professional capacity who, or any legal person which, through online intermediation services offers good or services to consumers for purposes relating to its trade, business, craft or profession*".

[159] Art. 2 (4) of the Platform-to-Business Regulation and Art. 2 (e) of the e-Commerce Directive define consumer as "*any natural person who is acting for purposes which are outside this person's trade, business, craft or profession*".

[160] Art. 5 of the e-Commerce Directive.

[161] Ibid., Art. 10 (1).

ECOM-4: Terms and conditions

KRAKEN should indicate any relevant terms and conditions to which it subscribes and information on how those codes can be consulted. The user should also be able to store and reproduce them.[162] When creating a KRAKEN user account, the user is prompted to read and accept the KRAKEN terms and conditions, which will also be made available through the KRAKEN website.

The terms and conditions must also: be drafted in plain and intelligible language, be easily available to business users at all stages of their commercial relationship with the service provider, set out the grounds for decisions to suspend or terminate or impose any other kind of restriction upon the provision of the service to business users, and include general information regarding the effects of the terms and conditions on the ownership and control of intellectual property rights of business users. In case of any changes to the terms and condition, business users must be notified[163]. Considering the scope of the Platform-to-Business Regulation, these requirements are in principle only applicable to business users making use of the KRAKEN platform. The current iteration of KRAKEN includes a KRAKEN Privacy Policy and an agreement between data providers and data consumers, but not yet the terms and conditions for the KRAKEN platform.

This requirement is dependent on the final adoption and exploitation of the KRAKEN platform, particularly on the identity and establishment of the entity that will provide the KRAKEN platform service. Depending on the Member State of establishment, different national obligations may also influence the specific contents of the terms and conditions.

ECOM-5: Liability exemption

The KRAKEN platform will benefit from the liability exemption for hosting services laid down in Article 5 of the upcoming DSA. Consequently, KRAKEN would not be liable for the information stored at the request of a recipient on the condition that the KRAKEN platform (a) does not have actual knowledge of illegal activity or illegal content and is not aware of facts or circumstances from which the illegal activity or illegal content is apparent; or (b) upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the illegal content. Actual knowledge or awareness could be obtained through a notice from a third party or by conducting voluntary own-initiative investigations, which would result in the KRAKEN platform having to take action against the illegal content.[164] It must also be reiterated that the KRAKEN platform does not store any data products (i.e., content data) of recipients, but rather stores information about that data product provided by those recipients. Consequently, the KRAKEN platform is not able to remove or disable access to the alleged illegal content itself, but rather to the information about that alleged illegal content.

ECOM-6: Monitoring obligation

Regarding content data, KRAKEN should not generally monitor the information which it transmits or stores, nor to actively seek facts or circumstances indicating illegal activity.[165] However, conducting voluntary own-initiative investigations and taking measures in good faith and in a diligent manner does not make KRAKEN ineligible for the liability exemption mentioned in this paragraph.[166]

ECOM-7: Provide an internal complaint-handling system

Under the Platform-to-Business Regulation, providers of intermediation services should provide an internal system for handling complaints of business users.[167]

[162] Ibid., Art. 10 (2) and (3).

[163] Art. 3 (1) and (2) of the Platform-to-Business Regulation.

[164] Recital 22 and Art. 6 DSA Proposal.

[165] Ibid., Art. 7.

[166] Ibid., Art. 6.

[167] Art. 11 of the Platform-to-Business Regulation.

Under the DSA, providers of online platforms must establish an easily accessible, user-friendly, and effective internal complaint-handling system that allows recipients of their service to lodge complaints against decisions taken upon the receipt of a notice or against decisions taken on the ground that the information provided by the recipients is illegal content or incompatible with its terms and conditions.[168]

Currently, KRAKEN has not yet implemented an internal complaint-handling system. However, users are able to contact KRAKEN in order to file a complaint against the decisions mentioned in the previous paragraph. This requirement should be further developed and implemented before the final adoption and exploitation of the KRAKEN platform.

3.5 Update on legal and ethical aspects of the pilots

The planned research activities of the pilots have undergone some changes since the submission of the WP8 ethics deliverables. In order to provide accurate and updated information, this section describes the research activities that have been performed in the pilots with regard to the involvement of human participants and the processing of personal data. More information on the methodological approach of the pilots can be found in D5.7 'KRAKEN marketplace testing and validation first report' and D5.8 'KRAKEN marketplace testing and validation final report'.

3.5.1 First pilot in October and November 2021

The first KRAKEN pilot involved limited user testing in the form of a workshop in Phase 1 (late October 2021) and an evaluation with group interviews in Phase 2 (beginning of November 2021).

3.5.1.1 Human participants

The participants of the first pilot were selected by the Bruno Kessler Foundation (FBK) through their professional networks and contacts and were limited to non-vulnerable adults that were able to give valid consent. The participants were generally individuals with competences in the relevant areas and were diversified to reflect different user groups and nationalities. For the educational pilot specifically, the Graz University of Technology (TUG) recruited mostly students from the TUG, with some external students and persons involved in the KRAKEN project as a back-up.

3.5.1.2 Processing of personal data

In Phase 1, for the testing purposes, participants were asked to create a user account on the KRAKEN platform using their own real personal data (i.e., first name, last name, e-mail address, over 18 years old, and country of residence). The participants were then asked to use this KRAKEN user account to publish and obtain fake personal data (i.e., dummy data) through the KRAKEN platform and subsequently rate its usability through an anonymous questionnaire. In Phase 2, for evaluation purposes, participants were invited to an evaluation session where group interviews were conducted. In this phase, there was limited processing of real personal data (i.e., name, gender, age group, e-mail address, occupation, video recording of the answers and comments regarding the KRAKEN evaluation). The processing of these categories of personal data were necessary to conduct the interviews, as well as gather the final research results.

For the educational pilot specifically, participants were presented with fake personal data (i.e., TUG test accounts) to log into the TUG portal. Once authorized, the system then exported fake personal data (i.e., fake student data) to the wallet of the participant. TUG also has an internal data protection policy that applies to the processing of personal data of students by TUG. Moreover, TUG obtains valid consent for the processing of personal data for student accounts and presents an information screen

[168] Art. 17 (1) and (2) DSA Proposal.

when users log into the TUG connector for the first time. This is not as relevant for the first pilot since TUG test accounts and fake student data were used.

The final evaluation results were anonymized to be presented in deliverables and presentations. The participants, as data subjects, were able to exercise their rights by contacting the appropriate KRAKEN contact person found on the informed consent sheet. The data protection policy of FBK also applied to the user testing and evaluation activities. This policy can be found on the FBK website and all FBK employees have attended a privacy course relating to data protection.

3.5.1.3 Informed consent

The KRAKEN informed consent sheets were adapted to the specific research activities of the first pilot. These consent sheets were presented to the participants prior to the start of the pilot activities and were aimed at informing the participants about their involvement in the pilot, the research activities, the research purposes, the processing of personal data, and their rights as data subjects. The informed consent sheets relating to the first pilot can be found in Annex A of D5.7 'KRAKEN marketplace testing and validation first report'.

3.5.1.4 Comments of the Ethics board

In D8.4.1 'Ethics board report', the Ethics board recommended making use of fake personal data in the pilots in order to avoid several concerns relating to the processing of real personal data. One of these concerns related to obtaining valid consent for the (further) processing of personal data in the biomedical pilot. Since, at the time D8.4.1 was submitted, it was planned to involve real hospitals with real personal data, the risks concerning valid informed consent were higher. The use of fake personal data allowed KRAKEN to avoid potential issues with informing the data subjects about the relevant data processing activities. In case real personal data was used, the hospital would have to check and verify the original consent of the data subjects to make sure it was in line with the research purposes and processing activities of the KRAKEN pilot.

Another concern of the Ethics board was the use of special categories of personal data in the pilot, since the GDPR follows a risk-based approach and these types of personal data enjoy a higher level of protection. This concern was also addressed by making use of fake personal data.

3.5.2 Final pilot in September 2022

The final KRAKEN pilot (September 2022) involved limited user testing in the form of a workshop in Phase 1 and an evaluation with individual interviews in Phase 2.

Although the organization of the final pilot was very similar to the first pilot, there are some differences in relation to the involvement of human participants and the processing of personal data.

3.5.2.1 Human participants

The participants of the final pilot were identified by FBK through a recruitment campaign in the KRAKEN network. Participants with different levels of expertise in the context of data sharing platforms were selected.

3.5.2.2 Processing of personal data

In Phase 1, for testing purposes, participants were asked to insert fake personal data to create an account on the KRAKEN platform. The only exception to the use of fake personal data was the e-mail address of the participant, which must be real and valid in order to test and evaluate the KRAKEN platform. In the biomedical pilot, participants were then asked to use this KRAKEN user account to publish and obtain anonymized personal data (i.e., non-personal data) through the KRAKEN platform. The anonymized personal data was sourced from a publicly available dataset, namely the Framingham study. In the educational pilot, participants were asked to use the KRAKEN user account to publish and obtain fake personal data (i.e., dummy data) through the KRAKEN platform. After performing these tasks, participants were asked to rate the usability through a questionnaire. The evaluation in Phase 2 of the final pilot was done through individual interviews with participants.

For the educational pilot specifically, as was the case in the first pilot, participants were presented with fake personal data (i.e., TUG test accounts) to log into the TUG portal. Once authorized, the system then exported fake personal data (i.e., fake student data) to the wallet of the participant.

The informed consent sheet relating to the final pilot can be found in Annex A of D5.8 'KRAKEN marketplace and testing validation final report'.

3.6 Recommendations

In general, the KRAKEN system fulfills the specified requirements. Certain requirements are at the moment not applicable yet, since they only become relevant for the final adoption and exploitation of the KRAKEN platform. Certain requirements are in principle fulfilled, but it could be further improved by implementing the following recommendations:

It would be useful, as also indicated in the feedback given on 31.5.2021 and on 1.3.2022, to provide a clear split in the user roles depending on whether the data provider is a data subject or a providing controller. This would simplify providing the correct information to the user, depending on the role they have.

To simplify the understanding of the users regarding what their obligations and rights are, but also how to correctly share the data, it would be useful to further add information in simple and clear language. An example of this is an explanation when the data provider has to indicate whether the provided data includes personal data or sensitive personal data, what exactly this entails and maybe also why this is important. Furthermore, the dashboard can be further extended with information and possibilities to exert data subject rights towards the receiving controller.

At the moment there is only a limited selection of possible purposes. This could be further extended, in order to allow a specific purpose indication instead of a general one. The best would be to include also an open indication of the purpose (in particular at the data consumer side), however, this seems to be technically not feasible at the moment.

While there is no issue regarding the transfer of the data to EU/EEA countries or countries with an adequacy decision, a data transfer to countries outside of the EU/EEA or countries without an adequacy decision is more problematic, as the data protection safeguards cannot be ensured. The KRAKEN system at the moment uses the derogation of art. 49 GDPR in the form of explicit consent, and provides a clear warning when selecting this option that it means that the GDPR safeguards will not apply, and this option should only be available to the data subject. Furthermore, it is intended that via contractual provisions the data consumer is obliged to nevertheless comply with the GDPR safeguards. Nevertheless, in practice this might not be sufficient to ensure a compliant processing, and it might be difficult to become aware of any non-compliant processing and to enforce the contract. This is related to a general issue, as KRAKEN can only provide the means to bring data providers and data consumers into contact with each other, but it is not possible to ensure that the data consumer complies with the GDPR provisions, only uses the data within the allowed timeframe, keeps it secure and does not use it for other purposes. Accordingly, in the promotion of the KRAKEN system, it should be avoided to give the impression to data subjects that the system would ensure the compliance of the data consumer regarding batch data. The use of the data analysis (SMPC) could be more favorable in this regard.

4 Lightweight development Data Protection Impact Assessment

The GDPR does not refer to a specific model for a DPIA, but states the minimum requirements for carrying out a DPIA.[169] A data protection impact assessment contains at least:

- a systematic description of the envisaged processing operations and the purposes of the processing, and in case the legitimate interest of the controller is considered the legal ground for processing, it also includes the legitimate interest;
- an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
- an assessment of the risks to the rights and freedoms of data subjects; and
- the measures envisaged to address the risks (e.g., safeguards and security measures).

Different national Data Protection Authorities (DPAs) have defined approaches and guidance for DPIAs. When analyzing the KRAKEN system, in particular the approach of the French Commission nationale de l'informatique et des libertés (CNIL)[170] and the German Standard Data Protection Model[171] have been taken into account. The analysis has been split along the lines of data processing that would take place in the context of the KRAKEN system: the processing of account data, the processing of batch data and the processing in the scope of data analytics. In line with the German Standard Data Protection Model, it also takes into account the different data protection goals. The full tables with the analysis can be found in the annex in the following tables: Table 5: DPIA table account data, Table 6: DPIA table batch data and Table 7: DPIA table data analytics. This chapter will only provide an overview of the results of the analysis, and the results from the stakeholder questions.

In the scope of the marketplace testing and validation, questions relating to the data protection approach and privacy heuristics were included. The full results can be found in KRAKEN Deliverable 5.7 and 5.8.[172]

In the scope of the first multi-dimensional evaluation, the questions regarding the data protection approach and potential risks were[173]:

- What is your impression of the level of data protection and privacy of the KRAKEN platform?
- Can you think of any data protection or privacy risks that you could encounter using the KRAKEN platform?
- Is the provided information relating to your data protection and privacy rights and freedoms sufficiently clear and understandable?
- Do you see any ethics concerns in using a data sharing platform like KRAKEN?

In the second evaluation, participants were asked “Is the provided information relating to your data protection and privacy rights and freedoms sufficiently clear and understandable?”.[174]

[169] Art. 35 (7) GDPR.

[170] See https://www.cnil.fr/en/privacy-impact-assessment-pia.

[171] Conference of the Independent Data Protection Supervisory Authorities of the Federation and the Länder, ‘The Standard Data Protection Model - A Method for Data Protection Advising and Controlling on the Basis of Uniform Protection Goals’, 17.4.2020.

[172] KRAKEN D5.7 ‘KRAKEN marketplace and validation first report’, 24.11.2021 and KRAKEN D5.8 ‘KRAKEN marketplace testing and validation final report’, 31.10.2022.

[173] KRAKEN D5.7 ‘KRAKEN marketplace testing and validation first report’, 16.

[174] KRAKEN D5.8 ‘KRAKEN marketplace testing and validation final report’, 19.

A part of the DPIA is the identification of planned or existing measures. Specific measures that are implemented in the KRAKEN system in order to minimize any data protection impacts are, for example, he use of security multi party computation for sharing encryption keys, and that the data is encrypted and stored under the control of the data subject in their preferred cloud storage. A dynamic consent function supports the data subject and allows it to set its preferences and to easily withdraw consent. The dashboard gives the data subject an overview of which data has been shared with which controller. Privacy metrics allow the data subject to decide how much data they want to publish while still be aligned with their privacy preferences. An idea is furthermore to establish a data provenance parameter to track the entire life cycle of a data product, including aggregated forms of the product derived from Data Unions or other data mergers. Finally, a data provider who is concerned about the security and privacy of their data assets can create a Data Product that is only available for analytics, whereby the SMPC nodes are located in the EU, and the result of the analytics is potentially anonymous.

The severity of the identified risks for KRAKEN acting as a controller for account data are all low. The severity of risks is based on the impact and likelihood of those risks, which are rather low considering the limited potential harm, small scale of processing activities, non-sensitive nature of the data, and implementation of technical and organizational measures. We conclude that the level of protection of the rights and freedoms of data subjects as well as the appropriate technical and organizational measures are sufficient to mitigate the identified risks.

It is not possible to identify the severity of the risks for the batch data and data analytics, as it depends upon the type of data that will be made available. However, considering the data protection measures taken by the KRAKEN platform, and in particular the possibility to use data analytics instead of sharing the data, the risks created by the system itself are considered in general to be rather low.

5 Self-sovereign identity

Self-sovereign identity started to surface in 2015 as the next solution for the missing identity layer of the internet.[175] The basic idea is that it is a decentralized and not account based identification solution. Even though there is no final consensus on what SSI is, generally the 10 principles defined by Christopher Allen are considered as the basic principles of SSI.[176] These principles are: 1) Users must have an independent existence; 2) Users must control their identities; 3) Users must have access to their own data; 4) Systems and algorithms must be transparent; 5) Identities must be long-lived; 6) Information and services about identity must be transportable; 7) Identities should be as widely usable as possible; 8) Users must agree to the use of their identity; 9) Disclosure of claims must be minimized; and 10) the rights of users must be protected.[177] As such it is not one specific system, but rather an approach which can be implemented in different ways.

An SSI solution is one of the three main pillars of the KRAKEN platform. For this, the KRAKEN project developed several components and subcomponents, which are explained in Deliverable 3.2.[178]

The following Verifiable Credential management tools components have been implemented in KRAKEN. The **Legal Identity Manager (LIM)**, which is for natural persons and can issue European Citizens a verifiable ID, named e-ID, derived from an eIDAS identity assertion. It furthermore, when acting as an SSI verifier, allows European citizens to sign documents with a signature certificate derived from their e-ID. More information can be found in Deliverable 3.2 section 3.1.

The **KRAKEN Web Company Tool (KWCT)** is a company “SSI general purpose” tool, which exchanges SSI transactions on a variety of use cases.[179] It operates on an identity wallet associated to a company, not a specific user. Two types of users can interact with the tool: external subjects and internal subjects. External subjects are users who do not belong to the organization that deploys the KWCT, while internal subjects are personnel belonging to the organization.[180]

To support the trust in the SSI solution, several services are developed.[181] The trust framework consists of the KRAKEN Trusted Issuer Registry (KTIR), KRAKEN Trusted Schema Registry (KTSR), KRAKEN Revocation & Endorsement Registry (KRER) and the KRAKEN Decentralized Identifier (DID) Registry.

A relying party must be able to trust the issuer of a credential, in order to trust a verifiable credential.[182] In KRAKEN, following the EBSI approach, for this the **KRAKEN Trusted Issuer Registry (KTIR)** is developed. The registry includes a list of issuers who are supposed to be trusted.[183]

[175] John Light, “How the BLOCKCHAIN Can Solve All Our (Identity) Problems,” in *Book of Proceedings IIWXX Internet Identity Workshop 20* (IIWXX, Computer History Museum, Mountain View, CA, 2015), 47; Kim Cameron, “The Laws of Identity,” 5.11.2005, https://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf; Alex Preukschat and Drummond Reed, “1. Why the Internet Is Missing an Identity Layer - and Why SSI Can Finally Provide One,” in *Self-Sovereign Identity*, ed. Alex Preukschat and Drummond Reed (Shelter Island: Manning, 2021), 6.

[176] Christopher Allen, “The Path to Self-Sovereign Identity,” Life With Alacrity, 25.4.2016, http://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html.

[177] Ibid.

[178] KRAKEN D3.2 ‘Self-Sovereign Identity Solution Final Release’, v1.0, 2.6.2022.

[179] Ibid., 18.

[180] Ibid., 20.

[181] Ibid., 24.

[182] Ibid., 24.

[183] Ibid., 24.

The content (set of claims) of a verifiable credential is defined by the verifiable credential's schema.[184] To support the schema definition and verification, the KRAKEN consortium implemented a minimal solution in the form of the **KRAKEN Trusted Schema Registry (KTSR)**. [185]

The **KRAKEN Revocation & Endorsement Registry (KRER)** includes information about the status of a verifiable credential, issuance and revocation dates, which is necessary for the verification of a verifiable credential.[186]

Finally, the **KRAKEN DID Registry** manages DIDs which are stored in the European Blockchain Services Infrastructure (EBSI).[187] The provided service by the European self-sovereign identity framework (ESSIF) is used to provide access to the DID document associated to a public DID stored by the EBSI/ESSIF DID registry. [188]

For the end user to use the SSI system, an application (**Ledger uSElf Mobile app**) has been designed and implemented to be run on their mobile phones.[189] To be user-friendly, the graphical user interface (GUI) and workflow of the application have been simplified.[190] To protect the identification data contained in the application, the access to it is protected by biometric authentication in the form of fingerprint or face recognition.[191] This biometric authentication takes place locally on the phone.

The previous D7.2 'Ethical and legal requirement specification' provided an overview of the relevant provisions of the eIDAS Regulation, and in how far they might be relevant for the SSI solution. With the upcoming Digital Identity Regulation, new relevant provisions might become applicable, which potentially also provide more business opportunities for the KRAKEN SSI system.

Regarding personal data, when a DID or a verifiable credential relates to a natural person, and not a legal person or a thing, it is considered to be personal data. Also revocation data which relates to a verifiable credential of a natural person constitutes personal data. While verifiable credentials are normally not stored on ledgers, DIDs and revocation information will often be stored on ledgers. In those cases, the issues explained below in section 6.1 are relevant, and the one processing the personal data needs to comply with the provisions of the GDPR.

[184] Ibid., 26.
[185] Ibid., 26.
[186] Ibid., 28.
[187] Ibid., 30.
[188] Ibid., 30.
[189] Ibid., 38.
[190] Ibid., 38.
[191] Ibid., 39.

6 Open issues and recommendations for policy-makers

This chapter sets out some of the open issues and challenges that we have encountered during the KRAKEN project. Based on the identified gaps and lessons learned these open issues can provide insights for potential policy recommendations.

6.1 The role and implications of blockchain in KRAKEN

KRAKEN uses blockchains at several places. Blockchains are used as verifiable data registry for the SSI solution, the xDai blockchain for payments, and the Lynkeus blockchain. In general, blockchain has certain features which are considered a challenge for compliance with data protection requirements. This entails in particular the decentralized nature and the immutability of the blockchain. Therefore, it is generally recommended to keep personal data off the blockchain.

However, even when avoiding the direct inclusion of personal data on the blockchain, there are open questions regarding the status of hashes and public keys.

A hash is the result of running input through a hashing function.[192] Hash functions are one-way functions, which means they are a method for a quick calculation with no known method to reverse the calculation.[193] What is important is the input to the hashing function, which can be personal data or not. In case the input is not personal data, then the resulting hash will normally also not be personal data, except if the hash is afterwards connected to identifying information of a natural person, which would make it personal data. For example, the hash of a license plate of a car owned by a legal person would in principle not be personal data. However, connecting it to a person driving it, at a specific time or in general, will make it personal data. In case personal data has been hashed, then it depends on several factors whether the resulting hash is considered anonymous or not. The Spanish DPA (AEPD) jointly with the European Data Protection Supervisor (EDPS) in their advice on hash functions[194] conclude that hash functions, though usually considered to only pseudonymize data, can under certain circumstances also be considered as anonymising personal data.[195] However, to be able to assume anonymization, a risk analysis must be done which results "in an objective assessment of the probability of re-identification in the long term" [196] This means, that for every hash function that would be used, such a risk assessment must be done, taking into account the basic elements listed by the AEPD.[197] Two important aspects to assume that the hash technique is an anonymization technique are the organizational measures which guarantee the removal of any information that allows for re-identification, and a reasonable guarantee of the system robustness beyond the expected useful life of the personal data. [198] The useful life expectancy of personal data can be more than 70 years, as it usually is the lifetime of the data subject.[199] Accordingly, in many cases it is the best to assume that hashes of personal data are still personal data.

It is still an open question whether public keys are personal data. Like hashing, public key cryptography and digital signatures are technologies that can be used with involvement of identifiable natural persons, or without. So, it depends on the implementation and use of the technology, whether public keys are considered personal data. For example, when using a digital signature to create an electronic

[192] Brent Zundel and Sajida Zouarhi, "6. Basic Cryptograph Techniques for SSI," in *Self-Sovereign Identity*, ed. Alex Preukschat and Drummond Reed (Shelter Island: Manning, 2021), 112.
[193] Zundel and Zouarhi, 113.
[194] AEPD (Spanish DPA) and EDPS, "INTRODUCTION TO THE HASH FUNCTION AS A PERSONAL DATA PSEUDONYMISATION TECHNIQUE," October 2019.
[195] AEPD (Spanish DPA) and EDPS, 22.
[196] Ibid., 22.
[197] Ibid., 23.
[198] Ibid., 23.
[199] Ibid., 22, though they refer to data holders instead of data subjects.

signature, which normally involves the use of a certificate which states that a certain public key belongs to a certain natural person (even though pseudonyms are allowed), the public key clearly constitutes personal data. Similarly, additional data can be connected in various ways to the public key, effectively making the data subject identifiable[200], and therefore, in many cases a public key can be considered as personal data. The difficulty is, that, while in some cases it may be clear that a public key constitutes personal data, in other cases it is not clear. However, even when a public key would in the beginning not be considered personal data, there would always be the risk that it could at some point of time become personal data. This would happen, as soon as it can be connected to an identified or identifiable natural person, which might even arise due to the actions of that person. This creates legal uncertainty, and means in essence that, in order to be on the safe side, public keys should in general be considered personal data. However, due to the ubiquitous use of public keys, this would create an unreasonable burden of compliance, since in many cases, with all the means reasonably likely to use, it will not be possible to relate the public key to a natural person. In case of blockchain, the French Data protection authority (DPA) CNIL considers that the public keys are essential to the blockchain's proper functioning.[201] Therefore it is not possible to minimise them and the retention period is in line with the lifetime of the blockchain. [202] However, the CNIL does not clarify, how data subjects rights can be complied with regarding public keys in the blockchain.

As will be explained in section 6.3, regarding the absolute and relative view on anonymization, clarification is necessary which view to follow and under which circumstances hashes and public keys can be assumed to not be personal data.

Another issue is the decentralized nature, which remains an open point of discussion that data protection role blockchain actors (users, miners, nodes) face. The general issue of allocation of roles and responsibilities under the GDPR will be explained in section 6.2, however, specifically for blockchain, the CNIL has specified that users can be considered controllers if the activity is either done by a legal person or a natural person which is not acting in the scope of a purely personal or household activity.[203] Miners are not considered to be controllers by the CNIL, as they do not define the purposes and means of the processing, but they might be considered processors.[204] Nodes are not considered in the analysis of CNIL, but other authors consider that nodes might be (joint) controllers.[205]

6.2 Roles and responsibilities under the GDPR

Under the GDPR, it is very important who the controller of the personal data processing is, as that entity is the one responsible for compliance with the provisions of the GDPR. The controller is the one, which "alone or jointly with others, determines the purposes and means of the processing of personal data".[206] Who the controller is, is a factual assessment, except if the controller has been identified by law. This means that whether somebody is a controller depends on the concrete activities in a specific

[200] See e.g., the examples given by Michèle Finck, "Blockchains and Data Protection in the European Union," *Max Planck Institute for Innovation and Competition Research Paper No. 18-01*, no. 18 (30.11.2017): 13, http://dx.doi.org/10.2139/ssrn.3080322.

[201] CNIL (Commission Nationale de l'Informatique et des Libertés), "Solutions for a Responsible Use of the Blockchain in the Context of Personal Data," September 2018, 7.

[202] Ibid., 7.

[203] Ibid., 1.

[204] Ibid., 2.

[205] See Michèle Finck, "Blockchain and the General Data Protection Regulation - Can Distributed Ledgers Be Squared with European Data Protection Law?" (Brussel, July 2019), 46–47, http://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf for an overview.

[206] Art. 4 (7) GDPR.

context.[207] The entity which has influence on the purposes and means of the processing is considered to be the controller. This also means that for example, an entity originally acting as a processor, can become a controller as soon as they do not follow the instructions of the controller but decide by themselves on the purposes and means of the personal data processing.

This factual approach has the consequence for KRAKEN that it is not possible to say with certainty which role the KRAKEN platform and the other actors will have. Small changes might result in a different assessment of the role of an entity, as it might be considered that the entity in that case decided on the purposes and means of the processing. However, a change of role without being aware of it, would have many consequences for the responsibility of the entity considering compliance with the GDPR.

Related to the question of which role an entity fulfills, is the question of joint controllership. The European Court of Justice (CJEU) judged on joint controllership in three recent decisions: *Wirtschaftsakademie*[208], *Jehovan todistajat*[209] and *Fashion ID*[210]. In all cases, the CJEU consistently reiterates the aim of the Data protection Directive to ensure a high level of protection of the fundamental rights and freedoms of natural persons[211], the fact that access to the personal data by every controller is irrelevant in case of joint controllership,[212] and that joint control does not mean equal responsibility[213]. In particular, the fact that it is not required for an entity to have access to the personal data in order to be considered a joint controller, could result in the status of joint controller while not being able to comply with the obligations of a controller. The EDPB considered in its guidelines that the status of joint controller can arise if the decisions controllers take are converging on purposes and means. [214] This happens, if they complement each other and "are necessary for the processing to take place in such manner that they have a tangible impact on the determination of the purposes and means of the processing"[215]. This can mean that it is possible that KRAKEN could be considered a joint controller, together with the receiving controller, simply due to the fact that the receiving controller might not have been able to receive the data if the KRAKEN service would not exist. However, it is not clear whether this is indeed the case, considering that the fact that the KRAKEN service exists, might not per se be considered a sufficiently "tangible impact" to become a joint controller. More guidance, legislation or clarifications in court could help to improve the legal certainty around the status of an intermediary data sharing service which does not have access to the shared data.

Finally, in the KRAKEN situation, but also more generally, for each new technology which aims to give data subjects more control, such as SSI and blockchain, the question of the status of a data subject as controller regarding its own personal data arises. This question is currently still discussed in the literature, but has not been clarified in the EDPB guidelines.[216] It is clear that natural persons can be

[207] European Data Protection Board, "Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR," 2.9.2020, 11.

[208] CJEU 5 June 2018, C-210/16, ECLI:EU:C:2018:388 ('*Wirtschaftsakademie* case').

[209] CJEU 10 July 2018, C-25/17, ECLI:EU:C:2018:551 ('*Jehovan todistajat* case').

[210] CJEU 29 July 2019, C-40/17, ECLI:EU:C:2019:629 ('*Fashion ID* case').

[211] First referred to in CJEU 13 May 2014, C-131/12, ECLI:EU:C:2014:317 (Google Spain), para 34; *Wirtschaftsakademie* case, para 28; *Jehovan todistajat* case, para 35; *Fashion ID* case, para 65-66.

[212] *Wirtschaftsakademie* case, para 38; *Jehovan todistajat* case, para 69; *Fashion ID* case, para 69 and 83.

[213] *Wirtschaftsakademie* case, para 43; *Jehovan todistajat* case, para 66; *Fashion ID* case, para 70 and 85.

[214] European Data Protection Board, "Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR," 18.

[215] Ibid., 18.

[216] Michèle Finck, "Cobwebs of Control: The Two Imaginations of the Data Controller in EU Law," *International Data Privacy Law* 11, no. 4 (December 20, 2021): 333–47, https://doi.org/10.1093/idpl/ipab017; Lokke Moerel, "Blockchain & Data Protection…and Why They Are Not on a Collision Course," *European Review of Private Law* 6 (2019): 825–52; European Data Protection Board, "Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR".

controllers when they process the personal data of other data subjects, such as in the *Lindqvist* and *Ryneš* cases.[217] The potential issues that arise from that will not be discussed here, as they mainly arise from the limited understanding and ability of normal users to comply with the data protection obligations.[218] The open question is, whether data subjects can be controllers of their own data, if they essentially define the purposes and means of the processing. However, this would mean that "the entire legal regime is turned on its head"[219]. The GDPR generally assumes the data subject and the controller to be different persons.[220] As one of the aims of the GDPR is to protect the data subject, it would also not make sense to protect the data subject from him/herself, except if the Regulation would be considered to take a rather paternalistic approach. Accordingly, it is unlikely that data subjects can be considered as controller for their own personal data. This, however, raises questions regarding the status of processors used by data subjects for their own personal data. In the case of KRAKEN, the issue can probably be avoided, since KRAKEN acts as controller for the account data, and for the content data no processing occurs until the receiving controller requests the data, which means that the receiving controller would be the controller for the ensuing processing.

6.3 The anonymization of personal data

The anonymization of personal data is another important topic that would benefit from additional clarification on the EU level. The application of the GDPR and its obligations depends on the qualification of data as personal data, which the GDPR defines as "*information relating to an identified or identifiable natural person*".[221] There are, however, ways to bring data outside the scope of the GDPR, for example by making use of anonymization techniques.

Under the GDPR, anonymous and pseudonymous data are two very different concepts. Anonymous data is data that "*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*".[222] Pseudonymous data, on the other hand, is data that "*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 organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person*".[223]

The important difference between these two concepts exists in the fact that pseudonymous data is still considered personal data and consequently triggers the material scope of the GDPR, while anonymous data is not considered personal data and therefore falls outside the scope of the GDPR. For data to be truly anonymous, the anonymization technique must be irreversible, which is generally difficult to attain.[224] In order to determine whether a person is identified or identifiable, and consequently whether the anonymization technique is truly irreversible, we must take into account "all the means reasonably likely to be used to identify the individual".[225]

The means "reasonably likely to be used to identify an individual" can be approached in two different ways. First there is the absolute approach, which assumes that the means to identify an individual can

[217] Judgement of 6. 11. 2003 — Case C-101/01 Bodil Lindqvist, No. C-101/01 (n.d.); Judgement of 11.12.2014— Case C-212/13 František Ryneš v Úřad pro ochranu osobních údajů, No. C-212/13 (n.d.).

[218] For more information on that, see Natali Helberger and Joris van Hoboken, "Little Brother Is Tagging You – Legal and Policy Implications of Amateur Data Controllers," *Computer Law Review International* 11, no. 4 (January 2010), https://doi.org/10.9785/ovs-cri-2010-101; Finck, "Cobwebs of Control."

[219] Finck, "Cobwebs of Control," 341.

[220] Ibid., 341.

[221] Art. 4 (1) of the GDPR.

[222] Ibid., Recital 26.

[223] Ibid., Article 4 (5).

[224] Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques, adopted on 10 April 2014, WP216, 6.

[225] Ibid., Recital 26.

be available to any third party, not just the controller. As a result, if any third party has the means to identify an individual, the data does not qualify as anonymous data under the absolute approach. This approach follows the wording of the GDPR and the relevant opinion of the Article 29 Working Party.[226] Secondly there is the relative approach, which states that only the perspective of the controller is important with respect to the means to identify an individual. Even though a third party may also have the means to identify an individual, as long as the controller does not have these means, the data would qualify as anonymous data under the relative approach. In essence, under the absolute approach, data can never qualify as anonymous for one party and as personal data for another party. For more information on what constitutes "means reasonably likely to be used", please see section 2.2.1.2 of D2.1 'Ethical and Legal Framework Report' and section 4.1.3 of D7.2 'Ethical and legal requirement specification'.

The question whether data can be considered anonymous becomes relevant for KRAKEN when we consider privacy-preserving data analysis as one of the services provided by the KRAKEN platform. In order to provide this service, KRAKEN employs SMPC to make computations over data and provide anonymous results to the data consumer. In this scenario, the results of SMPC can only be considered anonymous under the GDPR if the relevant individuals cannot be re-identified by making use of the means reasonably likely to be used. It is important to note that data still qualify as personal data before and during the anonymization process, up until the data have been fully anonymized. Collecting personal data for anonymization purposes and the anonymization process itself are therefore considered processing activities within the scope of the GDPR. In case the input data for SMPC constitute personal data, it follows that the GDPR applies until those input data have been fully anonymized. On the other hand, if the input data for SMPC do not constitute personal data, the GDPR will not apply to the input and output data.

It is also important to determine whether or not the output data can be considered anonymous under the GDPR. This assessment will depend on "the means that are reasonably likely to be used to re-identify individuals"; such as the costs and the amount of time required for re-identification, the available technology at the time of the processing, and technological developments.[227] In practice, such an assessment can only be made with sufficient technical expertise relating to the factors that determine whether the means "are reasonably likely to be used". Moreover, it is not required for re-identification to be completely impossible, but rather reasonably unlikely given the circumstances of the specific case and accompanying factors.[228]

Additionally, as described in section 6.1, the AEPD together with the European Data Protection Supervisor have jointly published advice on hash functions and anonymization. They conclude that hash functions, under certain circumstances, can be considered as anonymising personal data.

Considering the high threshold for full and irreversible anonymization as well as the relative nature of the "means reasonably likely to be used", it may be the case that organizations are under the belief certain data is anonymized, thereby falling outside the scope of the GDPR, while in reality it is not. It would therefore be beneficial to further clarify the concept of anonymization under the GDPR and provide more certainty to organizations employing anonymization techniques.

Another possibility to solve the differences between the absolute and the relative approaches would be the introduction of a third category of data, in between the concept of personal data and anonymous data. The issue regarding the two approaches is that under the absolute approach almost

[226] Ibid., Recital 26 states "*by the controller or by another person*"; and Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques, adopted on 10 April 2014, WP216, 5 and 6.
[227] Ibid., Recital 26.
[228] Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques, adopted on 10 April 2014, WP216, 8; and Data Protection Commission, Guidance Note: Guidance on Anonymisation and Pseudonymisation, June 2019, 5.

every data can become personal, even if the entity processing the data is not aware of it, while under the relative approach the protection of the GDPR is lost, which means that the data will not need to be secured and can easily end up in the hands of adversaries who can connect it to the data subject and create risks for their rights and freedoms. A potential solution would be to have a third category of data, in essence 'light touch personal data', in case the entity processing the data does not have the necessary means to relate it to an identifiable natural person, such as in the case of processing encrypted data without the key or imperfectly anonymized data without the means to re-identify. This 'light touch personal data' would not fall out of the scope of the GDPR as anonymous data would, but would have a reduced compliance burden under the GDPR, focusing on keeping the data secure and not sharing it with others who could potentially re-identify the data subject. It is worth considering whether this could be provided by an extended interpretation of art. 11 GDPR. Art. 11 GDPR entails that a controller, who processes data which does not require identification of a data subject by the controller, does not need to process additional data to identify the data subject in order to comply with the GDPR and the data subject rights provisions will not be applicable, except where the data subject provides additional information to enable the identification. It would need to be clarified which provisions need to be complied with when processing 'light touch personal data', and in which cases it would not be considered to be 'light touch personal data'. The EDPB is currently also working on their new guidelines on anonymization and pseudonymization, which will hopefully address some of the uncertainties.[229]

6.4 Consent as a legal basis

In KRAKEN, the publication and transfer of content by the data provider, as well as the processing of content data by the data consumer, is based on the legal basis of consent. Under the GDPR, consent is defined as "*any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her*".[230] Based on this definition, recital 32, as well as article 4 and 7 of the GDPR, we can identify some requirements for consent to be valid. This section will, however, not describe each of these requirements in detail, but will focus on the requirement of *informed* consent. More information on valid consent and its requirements can be found in section 2.2.3 of D2.1 'Ethical and Legal Framework Report' and section 4.3 of D7.2 'Ethical and legal requirement specification'.

In order for consent to be valid under the GDPR, it must be *informed*. To achieve this, the data subject must be properly informed prior to giving their consent. Informing the data subject should be done by providing easily accessible information in an intelligible way, using clear and plain language.[231] In case the data subject is not properly informed, they are unable to make informed decisions and fully understand what they are consenting to. The requirement of informed consent is therefore closely linked to the data protection principle of transparency.[232]

Informed consent requires a minimum of information to be provided to the data subject, which should include at least the following:[233]

- the identity and contact details of the controller;
- the purpose of each of the processing operations for which consent is obtained;
- what (types of) data will be collected and used;

[229] European Data Protection Board, EDPB Work Programme 2021/2022, 2.
[230] Art. 4 (11) of the GDPR.
[231] Ibid., Art. 7 (2).
[232] European Data Protection Board, Guidelines 05/2020 on consent Under Regulation 2016/679, 4 May 2020, 15.
[233] Recital 42 and Art. 7 (3), 13, and 14 of the GDPR; and European Data Protection Board, Guidelines 05/2020 on consent Under Regulation 2016/679, 4 May 2020, 15 – 16.

- the existence of the right to withdraw consent;
- information about the use of data for automated decision-making; and
- information on the possible risks of data transfers in the absence of an adequacy decision and of appropriate safeguards.

For a complete overview of the required information, articles 13 and 14 of the GDPR establish a list of information that should be provided to the data subject where personal data are collected from the data subject directly and indirectly.

A first question that becomes relevant for KRAKEN is whether it is sufficient to inform data subjects of the categories of controllers, rather than the specific identity of a controller. In KRAKEN, the consent flow is designed and implemented in such a way that allows for quick and automatic transactions on the marketplace. After a data provider publishes a data product on the KRAKEN platform, receiving controllers that are eligible under the specified conditions are able to automatically gain access to that data product. The advantage here is that, once a specific receiving controller wishes to access a data product, data providers do not have to approve that specific receiving controller. The question then arises whether consent can be considered informed when some of the necessary information, such as the identity of the controller, is not yet known at the time of obtaining consent. Even though the categories of controllers have been specified, the specific identity of the receiving controller has not. Taking into account the wording of recital 32 and articles 13 and 14 of the GDPR, as well as the opinion of the EDPB[234], it follows that such a consent would not be informed and thus invalid. KRAKEN has addressed this issue by presenting a list of pre-approved controllers to the data provider at the time of publishing a data product. In this way, the automatic nature of the consent process is not impaired and the data provider has the ability to pre-approve specific receiving controllers, thereby making the consent informed. This solution is effective in a scenario where the amount of listed controllers is limited, but could become burdensome in case there are too many controllers. It would also mean that, in order to be listed, controllers must have registered on the KRAKEN platform before the time of publication of a data product. Additional clarifications on the concept of informed consent would therefore be welcomed, specifically on the question whether consent is valid if the specific identity of the controller is not known at the time of consent, but the category of controller is known and the data protection principles and safeguards are guaranteed.

A second question that arises relates to the transfer of personal data from a primary controller to secondary controllers. Is consent considered informed when the identity of the primary controller is known, but potential secondary controllers are not yet identified? Particularly in the context of data markets, it is important to enable automatic transactions and potential transfers of data to secondary controllers. Following the GDPR, informed consent requires each secondary controller to obtain valid consent from the data subject for their own specific processing activities and purposes, thus creating additional hurdles for developing effective data markets. The EDPB has also stated that information on the identities of all secondary controllers who wish to rely on the original consent should be provided to the data subject. It is therefore implied that informing the data subject about the categories of secondary controllers would not suffice to obtain fully informed consent.[235] A potential solution to this issue would be the concept of transferable consent, where each secondary controller does not have to obtain new valid consent from the data subject. Transferable consent requires the primary controller to obtain valid consent from the data subject in such a way that establishes well-defined and specific conditions for the transfer of those personal data to potential secondary controllers. It is unclear whether transferable consent would be considered legitimate and valid under the GDPR, considering the requirement to inform the data subject of the identities of the secondary controllers. On the other hand, this approach is in line with the spirit of the GDPR and imposes that

[234] European Data Protection Board, Guidelines 05/2020 on consent Under Regulation 2016/679, 4 May 2020, 16.

[235] Ibid., 16.

the primary controllers may only transfer personal data in accordance with the well-defined and specific conditions of transfer as determined in the original consent, thereby staying within the boundaries of their legal basis. Once the identities of the secondary controllers are known, data subjects should be properly informed, for example by the primary controller.[236]

Finally, with regard to consent forms and as mentioned in section 2.1.11, the European Commission has planned to adopt implementing acts to establish a European data altruism consent form. This consent form will be GDPR-compliant and aims to provide a harmonized formal for consent and permissions across Member States.

6.5 The monetization of personal data

The concept of monetization of personal data is another open issue that requires further clarification and an official position by EU legislators and policy-makers.

Personal data is often used as a 'counter performance' or 'payment' for online services, which is becoming an increasingly common practice.[237] In this context, the French Supreme Administrative Court ruled that 'cookie walls' were not necessarily illegal in France and should be analyzed on a case-by-case basis.[238] This practice involves the offering of content on the condition that the data subject accepts non-essential cookies when using the service, which amounts to a payment in the form of personal data. There are, on the other hand, arguments to be made against the use of personal data in this way. Both the EDPS and EDPB have made clear that, in the EU, personal data cannot be considered as a mere economic asset or commodity.[239] The underlying reason for this stance is that "*even if the data subject can agree to the processing of his or her personal data, he or she cannot waive his or her fundamental rights*".[240] This reasoning has been reiterated by the EDPS and EDPB in 2021 and 2022, adding that "*this would not only undermine the very concept of human dignity and the human-centric approach the EU wants to uphold in its Data Strategy, but it would also risk undermining the rights to privacy and data protection as fundamental rights*".[241] The idea that personal data could be used as a counter performance is, however, not new in the EU landscape. Directives 2019/770 and 2019/2161, which cover digital services and consumer protection, mention the situation where a consumer provides personal data to a trader as a counter performance.[242]

In KRAKEN, personal data is not used as a counter performance or payment for online services. Data products, which may include personal data, are itself the subject of an exchange on the KRAKEN platform. Consequently, data providers give their valid consent for the processing of personal data in

[236] Bruegger Bud P., Transferable Consent as Enabler to Create Commons and Markets of Personal data; A discussion paper for PANELFIT WP3, limited distribution, 10-12.

[237] European Data Protection Supervisor, Opinion 8/2018 on the legislative package "A New Deal for Consumers", 5 October 2018, 3.

[238] Conseil d'Etat, Association des agences-conseils en communication & autres v CNIL, 19 June 2020 , nr. 434684.

[239] European Data Protection Board, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, Version 2.0, 8 October 2019, 15; and European Data Protection Supervisor, Opinion 8/2018 on the legislative package "A New Deal for Consumers", 5 October 2018, 12.

[240] European Data Protection Board, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, Version 2.0, 8 October 2019, 15.

[241] European Data Protection Board, Statement 05/2021 on the Data Governance Act in light of the legislative developments, adopted on 19 May 2021, 4; and European Data Protection Board and European Data Protection Supervisor, Joint Opinion 2/2022 on the Proposal of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act), adopted on 4 May 2022, 8 and 18.

[242] Art. 3 (1) of Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services; and Art. 4 (2) (b) of Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules.

exchange for a monetary value. The most notable difference with personal data as a counter performance exists in the fact that the data subject does not waive his or her fundamental rights, but rather consents to the processing of their personal data under restrictions and conditions specified by the data subject. For this approach to be considered legitimate, it is important that the KRAKEN platform allows its users to act in accordance with the GDPR, providing data providers and data consumers with relevant information on their obligations, providing a way to specify and adapt the valid consent given by data subjects, and enabling data subjects to exercise their rights. This approach was also confirmed by the German federal Data Protection Authority (Annex A), which emphasizes the need to ensure valid consent, transparency, and fair data protection principles. For more information on this approach, please see section 7.3.1 of D7.2 'Ethical and legal requirement specification'.

To conclude, there exists a need for further clarification and legislation on the concept of monetization of personal data and its consequences. Although the European strategy for data and digital services package aim to regulate the digital space and to create a single market for data, they lack in clearly and explicitly addressing the issues concerning data monetization in the online sphere.

7 Conclusion

This deliverable gave an overview in how far the ethical and legal requirements provided throughout the project have been taken into account. This includes an evaluation and validation of the ethical and legal requirements as well as recommendations to fill in the remaining gaps in implementation. Furthermore, this deliverable formulated further policy recommendations based on the identified gaps and lessons learned.

As there are several pieces of upcoming legislation that are of relevance for the KRAKEN project, the deliverable gave an overview of them, and in how far they might be relevant for KRAKEN. Firstly, the Data Governance Act (DGA) has been adopted and will apply from 24 September 2023. This act aims to foster availability of data for use by increasing trust in data intermediaries and by strengthening data-sharing mechanisms across the EU. The DGA is important for KRAKEN for its requirements for data intermediation service providers, providers of services of data cooperatives, and data altruism organizations. Secondly, there is the Data Act (DA), which is still in the proposal phase and awaiting committee decision. The DA aims to ensure fairness in the allocation of value from data among actors in the data economy and to foster access to and use of data. It could be important for KRAKEN for its obligations for data consumers and the possibility of data subjects to receive and share data generated by products and services. Thirdly, we have the Digital Identity Regulation (eIDAS 2.0), which is also still in the proposal phase and awaiting committee decision. It amends the eIDAS Regulation and includes, for example, European Digital Identity Wallets (EDIW) and extra trust services. It may be important for KRAKEN in relation to self-sovereign identity (e.g., EDIW and electronic attestations of attributes). Fourthly, there is the Digital Services Act (DSA), which has been adopted by the Council and is awaiting entry into force. It aims to establish a harmonized horizontal framework for due diligence, accountability, and transparency for providers of intermediary services according to their role, size, and impact in the online sphere. The DSA may be important for KRAKEN considering its layered obligations for intermediary service providers, hosting providers, and online platforms, as well as its rules on liability for hosting providers. Lastly, the Digital Markets Act (DMA) has also been adopted by the Council and is awaiting entry into force. It aims to level the playing field for all digital companies by complementing existing competition rules and defining clear rules for big platforms. It is most likely not important for KRAKEN considering the high threshold for applicability.

The evaluation and validation of the ethical and legal requirements is based on the requirements formulated in D7.2 'Ethical and legal requirement specification'. The evaluation of requirements covers the different capacities in which KRAKEN may act. These include KRAKEN as a controller for account data, KRAKEN as a data exchange service provider, KRAKEN as a data analytics provider, and KRAKEN as a provider of an information society service. Not all the identified requirements (e.g., some organizational requirements) are applicable or were able to be implemented during the development phase of the KRAKEN platform. Consequently, before final adoption and exploitation of the platform, certain requirements should be revisited and considered at a later stage. Moreover, some of the requirements that have been implemented could be further improved by following the recommendations formulated in section 3.6. The chapter on evaluation and validation also includes an update on the pilots that took place in 2021 and 2022, for which the KRAKEN consortium made changes in order to make use of fake personal data instead of real personal data where possible. As a result, many of the previously identified data protection risks have been mitigated.

Although not mandatory under the GDPR or soft-law guidelines, this deliverable also includes a lightweight development Data Protection Impact Assessment (DPIA). We conclude that the severity of the identified risks for the rights and freedoms of data subjects are rather low, which largely depends on the type of data in question (e.g., account data or content data). It is advised to conduct an additional risk assessment before the final adoption and exploitation of the KRAKEN platform, particularly with regard to content data.

Lastly, the deliverable provided information and an analysis of open issues that have been identified during the KRAKEN project. In particular, the role and implications of the use of blockchain, the roles and responsibilities under the GDPR, the anonymization of personal data, consent as a legal basis, and the monetization of personal data have been identified as areas in which further policy guidelines would be useful.

8 Bibliography

AEPD (Spanish DPA) and EDPS. "INTRODUCTION TO THE HASH FUNCTION AS A PERSONAL DATA PSEUDONYMISATION TECHNIQUE," October 2019.

Allen, Christopher. "The Path to Self-Sovereign Identity." Life With Alacrity, 25.4.2016. http://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereregin-identity.html.

Article 29 Data Protection Working Party. "Opinion 05/2014 on Anonymisation Techniques." adopted on 10 April 2014, WP216, 37 p.

Baloup, Julie, Emre Bayamlıoğlu, Aliki Benmayor, Charlotte Ducuing, Lidia Dutkiewicz, Teodora Lalova, Yuliya Miadzvetskaya, and Bert Peeters. "White Paper on the Data Governance Act." SSRN Electronic Journal, 2021. https://www.ssrn.com/abstract=3872703.

Bruegger, P. Bud. "Transferable Consent as Enabler to Create Commons and Markets of Personal data; A discussion paper for PANELFIT WP3." limited distribution, 17 p.

Cameron, Kim. "The Laws of Identity," 5.11.2005. https://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf.

CNIL (Commission Nationale de l'Informatique et des Libertés). "Solutions for a Responsible Use of the Blockchain in the Context of Personal Data," September 2018.

Conseil d'Etat. "Association des agences-conseils en communication & autres v CNIL." 19 June 2020, nr. 434684.

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "A European strategy for data," COM/2020/66 final, 19.2.2020. https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1593073685620&uri=CELEX%3A52020DC0066.

Data Protection Commission. "Guidance Note: Guidance on Anonymisation and Pseudonymisation." June 2019, 16 p.

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce').

Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital service.

Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules.

European Commission. "Commission Recommendation (2003/361/EC) of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises".

European Commission. "Digital Services Act: Commission welcomes political agreement on rules ensuring a safe and accountable online environment." https://ec.europa.eu/commission/presscorner/detail/en/IP_22_2545.

European Commission. "The Digital Services Act package." https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package.

European Council and Council of the European Union. "Digital services package." https://www.consilium.europa.eu/en/policies/digital-services-package/.

European Data Protection Board and European Data Protection Supervisor. "Joint Opinion 2/2022 on the Proposal of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act)." adopted on 4 May 2022, 28 p.

European Data Protection Board. "EDPB Work Programme 2021/2022." 6 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.” Version 2.0, 8 October 2019, 16 p.

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

European Data Protection Board. “Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR.” 2 September 2020, 48 p.

European Data Protection Board. “Statement 05/2021 on the Data Governance Act in light of the legislative developments.” adopted on 19 May 2021, 8 p.

European Data Protection Supervisor. “Opinion 8/2018 on the legislative package “A New Deal for Consumers.” 5 October 2018, 27 p.

European Parliament. “Briefing: EU Legislation in Progress: Digital services act.” https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689357/EPRS_BRI(2021)689357_EN.pdf.

Finck, Michèle. “Blockchain and the General Data Protection Regulation - Can Distributed Ledgers Be Squared with European Data Protection Law?” Brussel, July 2019. http://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf.

———. “Blockchains and Data Protection in the European Union.” Max Planck Institute for Innovation and Competition Research Paper No. 18-01, no. 18 (30.11.2017): 32. http://dx.doi.org/10.2139/ssrn.3080322.

———. “Cobwebs of Control: The Two Imaginations of the Data Controller in EU Law.” International Data Privacy Law 11, no. 4 (December 20, 2021): 333–47. https://doi.org/10.1093/idpl/ipab017.

Helberger, Natali, and Joris van Hoboken. “Little Brother Is Tagging You – Legal and Policy Implications of Amateur Data Controllers.” Computer Law Review International 11, no. 4 (January 2010). https://doi.org/10.9785/ovs-cri-2010-101.

Judgement of 6. 11. 2003 — Case C-101/01 Bodil Lindqvist, No. C-101/01 (n.d.).

Judgement of 11.12.2014 — Case C-212/13 František Ryneš v Úřad pro ochranu osobních údajů, No. C-212/13 (n.d.).

Light, John. “How the BLOCKCHAIN Can Solve All Our (Identity) Problems.” In Book of Proceedings IIWXX Internet Identity Workshop 20, 47. Computer History Museum, Mountain View, CA, 2015.

Moerel, Lokke. “Blockchain & Data Protection…and Why They Are Not on a Collision Course.” European Review of Private Law 6 (2019): 825–52.

Position of the European Parliament adopted at first reading on 5 July 2022 with a view to the adoption of Regulation (EU) 2022/… of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC.

Preukschat, Alex, and Drummond Reed. “1. Why the Internet Is Missing an Identity Layer - and Why SSI Can Finally Provide One.” In Self-Sovereign Identity, edited by Alex Preukschat and Drummond Reed, 3–19. Shelter Island: Manning, 2021.

Proposal for a Regulation of the European Parliament and of the Council Amending Regulation (EU) No 910/2014 as Regards Establishing a Framework for a European Digital Identity.” European Commission 2021/0136 (COD), 3.6.2021. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0281.

Proposal for a Regulation of the European Parliament and of the Council on harmonized rules on fair access to and use of data (Data Act), Pub. L. No. COM(2022) 68 final (23.3.2022).

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, Pub. L. No. OJ L 257/73, OJ L 257/73 (28.8.2014).

Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services.

Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act), OJ L 152/1, 3.6.2022." OJ L 152/1, n.d.

Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act).

Zundel, Brent, and Sajida Zouarhi. "6. Basic Cryptograph Techniques for SSI." In Self-Sovereign Identity, edited by Alex Preukschat and Drummond Reed, 111–25. Shelter Island: Manning, 2021.

Annexes

Requirements for KRAKEN as a controller of account data

Organizational (O) or technical (T) requirement	Obligation/Requirement	Done in KRAKEN?
DP-1 O/T Types of data	Identify the type of data which will be processed.	Account data is requested and collected when creating a KRAKEN user account: • first name, last name, e-mail address, country of residence, 18 years or older. Account data is limited to the types of data listed in the KRAKEN Privacy Policy and does not include special categories of personal data.
DP-2 O Roles	Define roles: identify who acts as controller and who acts as processor.	KRAKEN acts as the controller in relation to account data by determining the means and purposes of processing. The information on different roles is included in the KRAKEN Privacy Policy.
DP-2.1 *O*	IF controller-processor relationship: establish controller-processor agreement in writing.	N/A: there are no other parties that act as processors in relation to account data.
DP-2.2 *O*	IF joint controller relationship: establish joint controller agreement and make the essence of the arrangement available to the data subject.	N/A: KRAKEN is the sole controller in relation to account data.
DP-2.2.1 *O*	The joint controller agreement should include the allocation of respective responsibilities for compliance with the obligations under this Regulation, in particular: • exercising of the rights of the data subject and their respective duties to provide the information; and • designating a contact point for data subjects.	N/A: KRAKEN is the sole controller in relation to account data.
DP-3 O	Identify the purpose of the data processing.	The processing of account data is necessary to create and maintain a KRAKEN user account and make use of the

Organizational (O) or technical (T) requirement	Obligation/Requirement	Done in KRAKEN?
Purpose		KRAKEN platform service (i.e., to publish and make available a data product or obtain access to a data product on the KRAKEN platform). The processing of account data may also be necessary to comply with a legal obligation for the purpose of legal compliance, tax or auditing purposes, or to detect and prevent fraudulent or illegal activity.
DP-3.1 *O* *Re-use of data*	IF data is processed for another purpose AND not based on consent or legislation: controller must make an assessment on whether the processing is compatible with the purpose for which the personal data are initially collected.	N/A: KRAKEN does not process account data for purposes other than the original purposes listed in the Privacy Policy.
DP-4 O Legal Ground	Identify the legal ground of processing.	Account data is processed based on the necessity for the performance of a contract: account data are necessary for the performance of the contract between KRAKEN and the user, which exists in the creation and maintenance of a KRAKEN user account and the subsequent usage of the KRAKEN platform service. It may also be the case that KRAKEN processes account data based on a legal obligation (e.g., legal compliance, tax or auditing purposes, or to detect and prevent fraudulent or illegal activity).
DP-4.1 *O/T* *Consent*	IF the processing is based on consent: the controller must be able to demonstrate that the data subject has consented to processing of his or her personal data.	N/A: processing of account data is not based on the consent of the data subject.
DP-4.1.1 *O/T*	Consent must comply with the requirements of the GDPR.	N/A: processing of account data is not based on consent.
DP-4.1.2 *O/T*	Include the possibility to check that the person consenting is 18 years or older.	Although the processing of account data is not based on consent, in order to create a KRAKEN user account the user must state that they are 18 years or older.

Organizational (O) or technical (T) requirement	Obligation/Requirement	Done in KRAKEN?
DP-4.2 *O* *Legitimate interest*	IF the processing is based on the ground that it is necessary for the purposes of the legitimate interests pursued by the controller or by a third party: it must be ensured that the interests are not overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.	N/A: processing of account data is not based on the legitimate interests of the controller.
DP-4.3 *O/T*	IF special categories of personal data are processed: explicit consent needed.	N/A: account data does not include special categories of personal data.
DP-4.4 *O*	IF the processing is based upon the necessity for the performance of a contract: only process the data relevant for the contract.	The processing of account data is limited to personal data strictly necessary for the performance of the contract between KRAKEN and the user, which exists in the creation and maintenance of a KRAKEN user account and the subsequent usage of the KRAKEN platform service. Specific data such as the country of residence and 18 years or older is required to observe specific national legal obligations & requirements (e.g., national data protection provisions).
DP-5 O/T	Keep written records of processing activities.	The processing of account data by KRAKEN is limited in scope and the information on the processing activities related to account data are included in the KRAKEN Privacy Policy. The SSI and registration modules provide correspondent log files. Marketplace registration events are logged in the marketplace Backend database.
DP-5.1 *O*	Be able to make the written records available to the supervisory authority on request.	Information on the processing activities related to account data are included in the KRAKEN Privacy Policy. The log files related to SSI and user registration, product publication or product consumption within the marketplace can be made accessible to the supervisory authority.

Organizational (O) or technical (T) requirement	Obligation/Requirement	Done in KRAKEN?
DP-6 O/T Data subject rights	Facilitate the exercise of data subject rights.	Data subjects may contact KRAKEN to exercise their rights as a data subject in relation to account data. Information on how to exercise data subject rights and relevant contact details may be found in the KRAKEN Privacy Policy.
DP-6.1 *O/T*	Establish measures to easily retrieve information in case an access request or an audit is filed. Be able to: • inform the data subject whether or not personal data concerning him or her are processed; • provide a copy of the personal data (usually in electronic form) in a structured, commonly used and machine-readable format (to be able to comply with the right to data transfer); and • provide information.	KRAKEN is able to respond to access requests and provide the data subject with the necessary and relevant information. Relevant information may also be found in the KRAKEN Privacy Policy.
DP-6.2 *O/T*	Be able to stop the processing of personal data when a data subject request requires it.	By contacting KRAKEN, data subjects are able to object at any time to the processing of their account data for direct marketing purposes, which includes profiling to the extent that it is related to such direct marketing. Data subjects may also indirectly object to the processing of their account data by exercising their right to erasure (by deleting their KRAKEN user account through the KRAKEN user profile or by contacting KRAKEN).
DP-6.3 *O/T*	Be able to rectify the data without undue delay.	Data subjects are able to rectify their account data through the KRAKEN user profile or by contacting KRAKEN.
DP-6.4 *O/T*	Be able to communicate any rectification, erasure or restriction of processing to each recipient to whom the personal data have been disclosed.	Account data will never be transferred or made accessible to third parties, unless such a transfer is necessary to comply with a legal obligation, in which case KRAKEN should communicate any rectification, erasure or restriction to those recipients.

Organizational (O) or technical (T) requirement	Obligation/Requirement	Done in KRAKEN?
DP-6.5 *O/T*	Be able to erase the data without undue delay.	Data subjects are able to obtain the erasure of their account data by deleting their KRAKEN user account through the KRAKEN user profile or by contacting KRAKEN. As the information is kept on the Marketplace Registration VC which is under control of the user, the user can decide themselves how long the data should be made available. No personal data of the user is stored on the blockchain.
DP-6.5.1 *O/T*	IF the data was made public and must be erased due to a data subject request: take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.	Account data will never be transferred or made accessible to third parties, unless such a transfer is necessary to comply with a legal obligation. Account data will never be made publicly available.
DP-6.6 *O/T*	If automated individual decision-making is used: make sure the data subject is aware of it, has a possibility to object against it and provide the possibility to include a 'human in the loop'.	N/A: automated individual decision-making is not used in relation to account data.
DP-7 O Data Protection Policy	Implement a data protection policy.	For account data, KRAKEN implements a data protection policy through the KRAKEN Privacy Policy.
DP-8 O/T Information	Provide information to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language and in writing.	The KRAKEN Privacy Policy contains information relating to processing of account data in a concise, transparent, intelligible and easily accessible form, using clear and plain language. For additional information and questions regarding the processing of account data, data subjects may contact KRAKEN.
DP-9	Implement appropriate technical and organizational measures which are	KRAKEN implements technical and organizational measures to adhere to the

Organizational (O) or technical (T) requirement	Obligation/Requirement	Done in KRAKEN?
O/T Data protection by design	designed to implement data-protection principles in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.	requirements of the GDPR and to protect the rights of data subjects. Examples of measures are strong web security, end-to-end encryption, access & storage policies, and functionalities to easily exercise data subject rights.
DP-10 O/T Data protection by default	Implement appropriate technical and organizational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed.	KRAKEN, by default, only collects and processes account data that are strictly necessary for the listed purposes. The extent and period of processing of account data are also limited to what is strictly necessary for those purposes.
DP-11 O Data breach	In case of personal data breach which might result in a risk to the rights and freedoms of natural persons: notify without undue delay and if possible, no later than 72 hours after becoming aware of it to the competent supervisory authority.	In case of a data breach, KRAKEN should contact the supervisory authority to provide relevant and necessary information in accordance with article 33 GDPR.
DP-11.1 *O*	Document any personal data breach: the facts relating to the breach, its effects and the remedial actions taken.	In case of a data breach, KRAKEN should document the breach in accordance with article 33 (5) GDPR.
DP-11.2 *O*	In case of a personal data breach which might result in a high risk to the rights and freedoms of natural persons, communicate the breach in clear and plain language and without undue delay to the data subject.	Although a high risk to the rights and freedoms of natural persons is unlikely considering the types and non-sensitive nature of the account data in question, in such a case KRAKEN should communicate the breach to the data subject in accordance with article 34 GDPR.
DP-12 O DPIA	In case the processing is likely to result in a high risk to the rights and freedoms of natural persons: make a DPIA before the processing. If the result of the DPIA indicates a high risk: consult the supervisory authority.	N/A: the processing of account data by KRAKEN is not likely to result in a high risk to the rights and freedoms of natural persons considering the types, non-sensitive nature, and extent of processing activities.
DP-13 O	IF engaging a processor: only use processor providing sufficient guarantees to implement appropriate technical and organizational measures	N/A: KRAKEN is the sole controller in relation to account data. There are no other parties that act as processors in relation to account data.

Organizational (O) or technical (T) requirement	Obligation/Requirement	Done in KRAKEN?
Using Processor	in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.	
P-14 O/T Security	Establish technical and organizational security measures to deploy in the processing and storage of information.	The processing of account data is not likely to incur a high risk to the rights and freedoms of natural persons. Although this risk is low considering the types and non-sensitive nature of the account data in question, it is still important to implement appropriate technical and organizational security measures.
DP-14.1 *O/T*	Should implement pseudonymization and encryption of personal data.	KRAKEN implements end-to-end encryption to protect the confidentiality of data in transit.
DP-14.2 *O/T*	Should be able to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.	Measures such as strong web security, end-to-end encryption, and access & storage policies aim to protect confidentiality, integrity, availability, and resilience of systems and services.
DP-14.3 *O/T*	Should be able to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.	In case of an incident, KRAKEN can restore the availability of account data, which has a cloud backup, in a timely manner.
DP-14.4 *O/T*	Should have a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.	Technical and organizational security measures should be periodically tested and reviewed by KRAKEN.
DP-14.5 *O/T*	Should take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.	By implementing access policies and providing clear instructions, KRAKEN aims to limit processing of account data to what is necessary and instructed.
DP-15 O DPO	If necessary, designate a data protection officer and publish the contact details of the DPO and communicate them to the supervisory authority.	This requirement is not relevant for the processing of account data. However, in relation to content data, due to the potentially high volume of personal data, including special categories of personal data, the KRAKEN platform

Organizational (O) or technical (T) requirement	Obligation/Requirement	Done in KRAKEN?
		should designate a data protection officer and make their contact details available to the public and supervisor authority.
DP-16 O/T Third country Data Transfer	Only transfer personal data to a third country or an international organization if one of the conditions is given and therefore the level of protection guaranteed by the GDPR is not undermined: • transfer is on the basis of an adequacy decision; • transfer is subject to appropriate safeguards; • transfer is based on binding corporate rules; or • one of the derogations of art. 49 is applicable.	N/A: KRAKEN does not transfer account data to third countries or international organizations.

Table 1. Requirements for KRAKEN as a controller of account data

Requirements for KRAKEN as a data exchange service provider

Organizational (O) or technical (T) requirement	Obligation/Requirement	Done in KRAKEN?
DP-1 O/T Types of data	Identify the type of data which will be processed.	Data provider can indicate which data he provides.
DP-2 O Roles	Define roles: Identify who is controller and who processor.	Receiving controller: when buying access to the data, the screen shows an information that specifies that "by receiving and processing personal data you are considered a data controller under the General Data Protection Regulation and are consequently subject to its obligations. In particular, this includes that data subjects have the right to request from you the exercise of the data subject rights provided by the General data Protection Regulation, which includes: access to and rectification or erasure of their personal data, the restriction of or objection to the processing of their personal data, as well as the right to data portability. Data subjects also have the right to withdraw their consent at any time. For more information on the rights of the data subjects please consult KRAKEN's privacy policy".
DP-2.1 *O*	IF controller-processor relationship: establish controller-processor agreement in writing.	N/A
DP-2.2 *O*	IF joint controller relationship: establish joint controller agreement and make the essence of the arrangement available to the data subject.	N/A
DP-2.2.1 *O*	The joint controller agreement should include allocation of respective responsibilities for compliance with the obligations under this Regulation, in particular: - exercising of the rights of the data subject and their respective	N/A

Organizational (O) or technical (T) requirement	Obligation/Requirement	Done in KRAKEN?
	duties to provide the information; and - designate a contact point for data subjects.	
DP-3 O Purpose	Identify the purpose of the data processing.	When providing the data and when buying access to the data, the user interface requires to select purposes, and allows only access to the data when the purposes match. The selection of purposes is at the moment: Marketing, management or improvement of business services, publicly funded research, private research and automated decision-making, e.g., Artificial intelligence (including profiling).
DP-3.1 *O* *Re-use of data*	<u>IF data is processed for another purpose AND not based on consent or legislation</u>, controller must make an assessment on whether the processing is compatible with the purpose for which the personal data are initially collected.	Only in case data provider is another controller, outside of scope of KRAKEN.
DP-4 O Legal Ground	Identify the legal ground of processing.	Consent
DP-4.1 *O/T* *Consent*	<u>IF the processing is based on **consent**:</u> the controller must be able to demonstrate that the data subject has consented to processing of his or her personal data.	Data will only be provided with consent of the data subject who also defines the terms, which are stored and checked on the Lynkeus blockchain.
DP-4.1.1 *O/T*	Consent must comply with the requirements of the GDPR.	See requirements below.
	Indication of the data subject's wishes which signifies agreement to the processing of his/her personal data.	The consent must be an indication of the data subject's wishes which signifies agreement to the processing of his/her personal data. In the case of the provision of data via KRAKEN, this should normally apply, as the data subject actively provides the data, specifying the exact terms under which it will provide the data.

Organizational (O) or technical (T) requirement	Obligation/Requirement	Done in KRAKEN?
	Freely given	The consent must be freely given, which again, should be fulfilled as it is a free choice of the data subject to provide the data (the possibility exists that outside of the KRAKEN system users are coerced into providing the data, however, this is outside of the possibility for the KRAKEN system to detect. In such a case the consent will not be valid).
	Specific	The consent must also be specific and informed. In principle this is fulfilled, as the data subject can indicate who can receive which data, for how long and for which purposes. However, at the moment the selection of purposes is rather restricted, accordingly it would be better if, when the system would be further improved, to expand the potential purposes and/or add a free field.
	Informed	An open question is whether the data subject can be considered informed, if it does not know who will be processing his/her data at the moment of giving the consent. However, considering that the data subject is able to select who is allowed to process the data, and will get the required information in the dashboard as soon as the data consumer obtained access to the data, it is assumed that the data subject is sufficiently informed.
	Unambiguous	As it is the own action of the data subject which provides the access to the data, while clearly knowing and indicating for what the data may be used, the consent is unambiguous.
	Controller must demonstrate that the data subject has consented to the processing.	Via the Lynkeus blockchain it is only possible to receive access to the data when the information of the data consumer matches the requirements of the data provider. The consent will be stored on the blockchain and can be used

Organizational (O) or technical (T) requirement	Obligation/Requirement	Done in KRAKEN?
		to demonstrate that the data subject has consented to the processing.
	Possibility to withdraw consent at any time, must be as easy to withdraw as to give consent.	There must be a possibility to withdraw consent at any time, and it must be as easy to withdraw as to give consent. In the KRAKEN system this is possible via the marketplace mobile app, where the data subject has an overview of who has currently access to the data and an easy possibility to withdraw the consent.
	Before giving consent, the data subject must be informed that a withdrawal shall not affect the lawfulness of processing based on consent before its withdrawal.	Before giving consent, the data subject must be informed that a withdrawal shall not affect the lawfulness of processing based on consent before its withdrawal.
DP-4.1.2 *T/O*	Include possibility to check that the person consenting is over 18.	At sign up, the person signing up has to confirm that they are over 18.
DP-4.2 *O* *Legitimate interest*	<u>IF the processing is based on the ground that it is necessary for the purposes of the **legitimate interests pursued by the controller** or by a third party</u>: it must be ensured that the interests are not overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.	N/A
DP-4.3 *O/T*	<u>IF special categories of personal data are processed</u>: explicit consent needed.	Though it would only be necessary when the data provider indicates that the data includes special categories of data, nevertheless, the consent is done in such a way that normally the requirements for explicit consent are always fulfilled, since the data subject has to actively provide the data and the requirements for consent and can select who might receive the data.
DP-4.4 *O*	<u>IF the processing is based upon contract</u>: only process the data relevant for the contract.	N/A

Organizational (O) or technical (T) requirement	Obligation/Requirement	Done in KRAKEN?
DP-5 O/T	Keep written records of processing activities.	N/A: obligation for the receiving controller.
DP-5.1 *O*	Be able to make the written record available to the supervisory authority on request.	N/A: obligation for the receiving controller.
DP-6 O/T Data subject rights	Facilitate the exercise of data subject rights.	As the KRAKEN system does only facilitate the exchange but is not involved in the actual processing, the exercise of data subject rights depends on the receiving controller, who must be able to comply with the obligations. The KRAKEN system can facilitate the exercise of data subject rights, by giving the data subject an easy way to exercise their data subject rights to the receiving controller via the dashboard.
DP-6.1 *O/T*	Establish measures to easily retrieve information in the case an access request or an audit is filed. Be able to: • inform the data subject whether or not personal data concerning him or her are processed; • provide a copy of the personal data (usually in electronic form). Also in a structured, commonly used and machine-readable format (to be able to comply with the right to data transfer); and • provide information.	In principle N/A since it is an obligation for the receiving controller. Information is provided via the dashboard.
DP-6.2 *O/T*	Be able to stop the processing of personal data when a data subject request requires it.	In principle N/A since it is an obligation for the receiving controller. Information on how to contact the controller to use data subject rights is available via the dashboard.
DP-6.3 *O/T*	Be able to rectify the data without undue delay.	In principle N/A since it is an obligation for the receiving controller. Information on how to contact the controller to use data subject rights is available via the dashboard.

Organizational (O) or technical (T) requirement	Obligation/Requirement	Done in KRAKEN?
DP-6.4 *O/T*	Be able to communicate any rectification, erasure or restriction of processing to each recipient to whom the personal data have been disclosed.	In principle N/A since it is an obligation for the receiving controller. Information on how to contact the controller to use data subject rights is available via the dashboard.
DP-6.5 *O/T*	Be able to erase the data without undue delay.	In principle N/A since it is an obligation for the receiving controller. Information on how to contact the controller to use data subject rights is available via the dashboard.
DP-6.5.1 *O/T*	IF the data was made public and must be erased due to a data subject request: take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.	In principle N/A since it is an obligation for the receiving controller. Information on how to contact the controller to use data subject rights is available via the dashboard.
DP-6.6 *O/T*	If automated individual decision-making is used: make sure the data subject is aware of it, has a possibility to object against it and provide the possibility to include a 'human in the loop'.	In case automated decision making is used, it must be possible to make sure the data subject is aware of it, provide a possibility to object against it and provide the possibility to include a 'human in the loop'. The data provider is aware of the processing, as he can select whether or not he agrees with the use of the data for automated decision making and can simply object against it by not making it available for this purpose. When the data provider indicates the agreement with the automated decision making purpose, he also needs to indicate which workings and potential significance and envisaged consequences of automated decision making are approved: automated placing of services and product offerings, hiring assessments, clinical risks assessment, diagnostic or treatment suggestions.

Organizational (O) or technical (T) requirement	Obligation/Requirement	Done in KRAKEN?
		The possibility to include a 'human in the loop' is a requirement that needs to be fulfilled at the receiving controller's side.
DP-7 O Data Protection Policy	Implement a data protection policy.	N/A
DP-8 O/T Information	Provide **information** to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language and in writing.	It is aimed for to provide the information to the data subject in a clear and easily accessible form. With a split in data provision between data subject and providing controller, this would be easier. More detailed information can be provided, but this was not in the scope of the current work for the UI.
DP-9 O/T Data protection by design	Implement appropriate technical and organizational measures which are designed to implement data-protection principles in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.	The KRAKEN system gives the data subject the possibility to indicate which data under which circumstances might be processed by which entity. Furthermore, it gives the possibility to encrypt the batch data in order to keep it secure and avoid access from data consumers which do not fulfill the requirements set out by the data subject.
DP-10 O/T Data protection by default	Implement appropriate technical and organizational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed.	It is not possible for KRAKEN to verify whether the provided personal data is indeed necessary for the indicated purpose. It is expected that the data subject and data consumer only indicate to share data which is necessary for the indicated purpose, whereby it would be recommended to extend the selection of purposes.
DP-11 O Data breach	In case of personal data breach which might result in a risk to the rights and freedoms of natural persons: notify without undue delay and if possible, no later than 72 hours after becoming aware of it to the competent supervisory authority.	N/A

Organizational (O) or technical (T) requirement	Obligation/Requirement	Done in KRAKEN?
DP-11.1 *O*	Document any personal data breach: the facts relating to the breach, its effects and the remedial actions taken.	N/A
DP-11.2 *O*	In case of a personal data breach which might result in a high risk to the rights and freedoms of natural persons, communicate the breach in clear and plain language and without undue delay to the data subject.	N/A
DP-12 O DPIA	In case the processing is likely to result in a high risk to the rights and freedoms of natural persons: make a DPIA before the processing. If the result of the DPIA indicates a high risk: consult the supervisory authority.	N/A
DP-13 O Using Processor	IF engaging a processor: only use processor providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.	N/A
DP-14 O/T Security	Establish technical and organizational security measures to deploy in the processing and storage of information.	KRAKEN provides encryption of the batch data and does not keep the data at its system. The product publication and product consumption processes can only be completed if the data product has been encrypted and decrypted in the marketplace Frontend. Accordingly, the security requirements are not for the KRAKEN system but for the receiving controller.
DP-14.1 *O/T*	Could use pseudonymization and encryption of personal data.	KRAKEN provides encryption of the data.
DP-14.2 *O/T*	Should be able to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.	KRAKEN provides encryption of the batch data and does not keep the data at its system. Accordingly, the security requirements are not for the KRAKEN system but for the receiving controller.
DP-14.3 *O/T*	Should be able to restore the availability and access to personal data	KRAKEN provides encryption of the batch data and does not keep the data at its

Organizational (O) or technical (T) requirement	Obligation/Requirement	Done in KRAKEN?
	in a timely manner in the event of a physical or technical incident.	system. Accordingly, the security requirements are not for the KRAKEN system but for the receiving controller.
DP-14.4 *O/T*	Should have a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.	During the development the system is tested, however, when the system is implemented a process for regularly testing, assessing and evaluating the measures would need to be established. This, in particular, to make sure that the encryption if functioning, and personal data will not become available to anybody except the encryption service for the purpose of encrypting the data.
DP-14.5 *O/T*	Should take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.	This is a requirement for after establishment of the KRAKEN platform, to ensure the encryption is secure and working correctly, however, as the data is not kept at the KRAKEN platform, it will general not be applicable.
DP-15 O DPO	<u>If necessary</u>, designate a data protection officer and publish the contact details of the DPO and communicate them to the supervisory authority.	N/A
DP-16 O/T Third country Data Transfer	Only transfer personal data to a third country or an international organization if one of the conditions is given and therefore the level of protection guaranteed by the GDPR is not undermined: • transfer is on the basis of an adequacy decision; • transfer is subject to appropriate safeguards; • transfer is based on biding corporate rules; or • one of the derogations of art. 49 is applicable.	This requirement provides that personal data may only be transferred to a third country or an international organization if one of the conditions is given and therefore the level of protection guaranteed by the GDPR is not undermined: • transfer is on the basis of an adequacy decision; • transfer is subject to appropriate safeguards; • transfer is based on biding corporate rules; or • one of the derogations of art. 49 is applicable. In the KRAKEN system, the data provider can indicate to which countries the data may be transferred. This is done by

Organizational (O) or technical (T) requirement	Obligation/Requirement	Done in KRAKEN?
		indicating at the question to which country and region may the data be transferred, whether they allow a transfer to EU/EEA countries, non-EU/EEA country with an adequacy decision, or non-EU/EEA country without an adequacy decision. In the last case, a warning applies that if this option is chosen, there will be no safeguards from the GDPR applying to the processing. In the agreement is specified that the data consumer has to comply with the GDPR. A potential problem with that solution is, however, that the data subject might not be able to sue the receiving controller in case of a breach of contract. Accordingly, it might be worth considering not to include non-EU/EEA countries without an adequacy decision, except if it could be validated in some way that they provide an equivalent level of protection to the GDPR.

Table 2: Requirements for KRAKEN as data exchange service provider

Requirements for KRAKEN as data analytics provider

Organizational (O) or technical (T) requirement	Obligation/Requirement	Done in KRAKEN?
DP-1 O/T Types of data	Identify the type of data which will be processed.	The User Interface requests whether the provided data entails personal data and whether it is sensitive personal data. It would be useful to add information on what is personal data and special categories of personal data, to enable the data provider to provide correct information.
DP-2 O Roles	Define roles: Identify who is controller and who processor.	Not entirely clear, as it depends on the factual circumstances. Assume that KRAKEN will be acting as a processor in the case of providing analytic services, and the SMPC nodes might be considered sub-processors.
DP-2.1 *O*	IF controller-processor relationship: establish controller-processor agreement in writing.	N/A as it is an organizational requirement.
DP-2.2 *O*	IF joint controller relationship: establish joint controller agreement and make the essence of the arrangement available to the data subject.	N/A as processor.
DP-2.2.1 *O*	The joint controller agreement should include allocation of respective responsibilities for compliance with the obligations under this Regulation, in particular: • exercising of the rights of the data subject and their respective duties to provide the information; and • designate a contact point for data subjects.	N/A as processor.
DP-3 O Purpose	Identify the purpose of the data processing.	The purpose of the processing is the encryption to be then analyzed in a secure and privacy friendly manner, resulting in presumably anonymous data.
DP-3.1 *O*	IF data is processed for another purpose AND not based on consent or legislation, controller must make an	N/A as processor.

Organizational (O) or technical (T) requirement	Obligation/Requirement	Done in KRAKEN?
Re-use of data	assessment on whether the processing is compatible with the purpose for which the personal data are initially collected.	
DP-4 O Legal Ground	Identify the legal ground of processing.	The data subject consents to the encryption and analysis. The result is presumed not to be personal data, therefore no legal ground is necessary. If data subject provides data, consent is obtained directly by the system, if data provider is not data subject, he must have ensured that the data subject consents to this processing.
DP-4.1 *O/T* *Consent*	IF the processing is based on **consent**: the controller must be able to demonstrate that the data subject has consented to processing of his or her personal data.	N/A as processor.
DP-4.1.1 *O/T*	Consent must comply with the requirements of the GDPR.	N/A as processor.
DP-4.1.2 *T/O*	Include possibility to check that the person consenting is over 18.	Is included, UI asks upon registration whether the person is above 18. Due to the fact that the UI have not been split into DS version and providing controller version: not clear if it is ensured that the data subjects consenting to the sharing of their data by the providing controller are above 18. This is, however, not per se necessary, as they can according to the GDPR also be below 18, the important aspect is that the consent which was provided to the providing controller is valid. This is, however, outside of the scope of the KRAKEN system.
DP-4.2 *O* *Legitimate interest*	IF the processing is based on the ground that it is necessary for the purposes of the **legitimate interests pursued by the controller** or by a third party: it must be ensured that the interests are not overridden by the interests or fundamental rights and freedoms of the data subject which require protection of	N/A as processor.

Organizational (O) or technical (T) requirement	Obligation/Requirement	Done in KRAKEN?
	personal data, in particular where the data subject is a child.	
DP-4.3 *O/T*	IF special categories of personal data are processed: explicit consent needed.	N/A as processor.
DP-4.4 *O*	IF the processing is based upon contract: only process the data relevant for the contract.	N/A as processor.
DP-5 O/T	Keep written records of processing activities.	N/A: DP-21.
DP-5.1 *O*	Be able to make the written record available to the supervisory authority on request.	N/A: DP-21.
DP-6 O/T Data subject rights	Facilitate the exercise of data subject rights.	N/A: DP-17.
DP-6.1 *O/T*	Establish measures to easily retrieve information in the case an access request or an audit is filed. Be able to: • inform the data subject whether or not personal data concerning him or her are processed; • provide a copy of the personal data (usually in electronic form). Also in a structured, commonly used and machine-readable format (to be able to comply with the right to data transfer); and • provide information.	N/A: DP-17.
DP-6.2 *O/T*	Be able to stop the processing of personal data when a data subject request requires it.	N/A: DP-17.
DP-6.3 *O/T*	Be able to rectify the data without undue delay.	N/A: DP-17.
DP-6.4 *O/T*	Be able to communicate any rectification, erasure or restriction of	N/A: DP-17.

Organizational (O) or technical (T) requirement	Obligation/Requirement	Done in KRAKEN?
	processing to each recipient to whom the personal data have been disclosed.	
DP-6.5 *O/T*	Be able to erase the data without undue delay.	N/A: DP-17.
DP-6.5.1 *O/T*	IF the data was made public and must be erased due to a data subject request: take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.	N/A as processor.
DP-6.6 *O/T*	If automated individual decision-making is used: make sure the data subject is aware of it, has a possibility to object against it and provide the possibility to include a 'human in the loop'.	N/A as processor.
DP-7 O Data Protection Policy	Implement a data protection policy.	N/A as processor.
DP-8 O/T Information	Provide **information** to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language and in writing.	N/A as processor.
DP-9 O/T Data protection by design	Implement appropriate technical and organizational measures which are designed to implement data-protection principles in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.	N/A as processor.
DP-10 O/T Data protection by default	Implement appropriate technical and organizational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed.	N/A as processor.

Organizational (O) or technical (T) requirement	Obligation/Requirement	Done in KRAKEN?
DP-11 O Data breach	In case of personal data breach which might result in a risk to the rights and freedoms of natural persons: notify without undue delay and if possible, no later than 72 hours after becoming aware of it to the competent supervisory authority.	N/A: DP-22.
DP-11.1 *O*	Document any personal data breach: the facts relating to the breach, its effects and the remedial actions taken.	N/A: DP-22.
DP-11.2 *O*	In case of a personal data breach which might result in a high risk to the rights and freedoms of natural persons, communicate the breach in clear and plain language and without undue delay to the data subject.	N/A: DP-22.
DP-12 O DPIA	In case the processing is likely to result in a high risk to the rights and freedoms of natural persons: make a DPIA before the processing. If the result of the DPIA indicates a high risk: consult the supervisory authority.	N/A as processor.
DP-13 O Using Processor	IF engaging a processor: only use processor providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.	N/A: DP-19.
DP-14 O/T Security	Establish technical and organizational security measures to deploy in the processing and storage of information.	See answers below.
DP-14.1 *O/T*	Could use pseudonymization and encryption of personal data.	Since the processing that KRAKEN provides is actually the splitting of the personal data into shares, encrypting, and analysing them, after which they are given to the data consumer, this requirement is fulfilled.
DP-14.2 *O/T*	Should be able to ensure the ongoing confidentiality, integrity, availability and	As the key shares are shared to the SMPC nodes, and each SMPC node only receives a part of the data, the

Organizational (O) or technical (T) requirement	Obligation/Requirement	Done in KRAKEN?
	resilience of processing systems and services.	confidentiality is ensured. Integrity, availability, and resilience are the responsibility of the data provider, as KRAKEN has not access to the full dataset.
DP-14.3 *O/T*	Should be able to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.	As KRAKEN sends the encrypted data to the data consumer, it is not possible to restore the availability or access to personal data afterwards, as it is not located at the KRAKEN platform anymore and becomes the responsibility of the data consumer after it has been given back to them.
DP-14.4 *O/T*	Should have a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.	During the development the system is tested, however, when the system is implemented a process for regularly testing, assessing and evaluating the measures would need to be established. This in particular to make sure that the encryption if functioning, and personal data will not become available to anybody except the encryption service for the purpose of encrypting the data.
DP-14.5 *O/T*	Should take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.	As the encryption, though provided by KRAKEN, takes place at the side of the data provider, normally no natural person working for KRAKEN would have access to the data.
DP-15 O DPO	If necessary, designate a data protection officer and publish the contact details of the DPO and communicate them to the supervisory authority.	As an organizational requirement, this is currently not applicable and will only be necessary to be fulfilled when the KRAKEN platform acts in the market.
DP-16 O/T Third country Data Transfer	Only transfer personal data to a third country or an international organization if one of the conditions is given and therefore the level of protection guaranteed by the GDPR is not undermined:	As the SMPCs and the KRAKEN platform are all located within the European Union, and the result of the analysis is considered to be anonymous, this requirement is not applicable.

Organizational (O) or technical (T) requirement	Obligation/Requirement	Done in KRAKEN?
	• transfer is on the basis of an adequacy decision; • transfer is subject to appropriate safeguards; • transfer is based on biding corporate rules; or • one of the derogations of art. 49 is applicable.	
DP-17 O/T	Provide sufficient guarantees to implement appropriate technical and organizational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.	The only processing in this scope is the encryption of the data for the SMPC analytics. When complying with the requirements set out here, it will be assumed that this requirement will be fulfilled.
DP-18 O	Don't engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.	As an organizational requirement this is not applicable at the moment, however, whether it will be relevant in the exploitation of KRAKEN will depend on whether the SMPCs will be considered as sub-processors or not.
DP-19 O	IF the processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor shall be imposed on that other processor by way of a contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of this Regulation.	As an organizational requirement, it is not applicable at the moment.
DP-20 O	Only process data upon instructions of the controller (except required to do so by Union or Member State law).	As an organizational requirement, it is not applicable at the moment.

Organizational (O) or technical (T) requirement	Obligation/Requirement	Done in KRAKEN?
DP-21 O/T	Keep a written record of all categories of processing activities.	The only processing activity taking place is the encryption of the data, which is not an ongoing processing activity, but only an incidental one, and the data is not kept by the KRAKEN platform.
DP-22 O	Notify controller in case of a data breach.	As an organizational requirement, it is not applicable at the moment.

Table 3: Requirements for KRAKEN as data analytics provider

Requirements for KRAKEN as a provider of an information society service

Requirement	Obligation	Done in KRAKEN?
ECOM-1	Establish whether the user is acting as a consumer or a business user.	The current KRAKEN UI does not include the possibility for a user to signify whether they are acting as a business user or as a consumer for a given transaction. Even though this requirement has not been fulfilled at this point in time, it is still possible to satisfy the other requirements that result from the qualification as a business user or as a consumer (e.g., terms and conditions in plain and intelligible language, easily available, etc.).
ECOM-2	Include easily reachable information on the service provider.	This requirement is dependent on the final adoption and exploitation of the KRAKEN platform, particularly on the identity and establishment of the entity that will provide the KRAKEN platform service. Consequently, this requirement should be implemented at the time such information is available.
ECOM-3	Provide information for the conclusion of a contract with a consumer.	The KRAKEN UI guides the user through the different steps in order to publish or obtain access to a data product. Prior to placing the order, the user is able to identify and correct any input errors by assessing the final overview page of the order. The contract between KRAKEN and the user is concluded by publishing or obtaining access to a data product as well as accepting the Terms and conditions of the KRAKEN platform.
ECOM-4	Terms and conditions.	When creating a KRAKEN user account, the user is prompted to read and accept the KRAKEN terms and conditions, which will also be made available through the KRAKEN website. The current iteration of KRAKEN includes a KRAKEN Privacy Policy and an agreement between data providers and data consumers, but not yet the terms and conditions for the KRAKEN platform. This requirement is dependent on the final adoption and exploitation of the KRAKEN platform, particularly on the identity and establishment of the entity that will provide the KRAKEN platform service. Depending on the Member State of establishment, different national obligations may also influence the specific contents of the terms and conditions.
ECOM-5	Liability exemption.	KRAKEN would not be liable for the information stored at the request of a recipient on the condition that the KRAKEN platform (a) does not have actual knowledge of illegal activity or illegal content and is not aware of facts or circumstances from which the illegal activity or illegal content is apparent; or (b) upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the illegal content (art. 14 e-Commerce Directive and art. 5 DSA). Actual knowledge or awareness could be obtained through a notice from a third party or by conducting voluntary own-

Requirement	Obligation	Done in KRAKEN?
		initiative investigations, which would result in the KRAKEN platform having to take action against the illegal content (art. 6 DSA).
ECOM-6	Monitoring obligation.	Regarding content data, KRAKEN should not generally monitor the information which it transmits or stores, nor to actively seek facts or circumstances indicating illegal activity (art. 15 e-Commerce Directive and art. 7 DSA).
ECOM-7	Provide an internal complaint-handling system.	Currently, KRAKEN has not yet implemented an internal complaint-handling system. However, users are able to contact KRAKEN in order to file a complaint against the decisions mentioned in the previous paragraph. This requirement should be further developed and implemented before the final adoption and exploitation of the KRAKEN platform.

Table 4: Requirements for KRAKEN as a provider of an information society service

DPIA table account data

Question	Answer	Comments
Context		
What is the processing under consideration?	The processing under consideration is the creation and maintenance of a KRAKEN user account. In order to make use of the KRAKEN platform service (i.e., to publish and make available a data product or obtain access to a data product) users must create a KRAKEN user account by signing up and providing the necessary account data. Only natural persons can register on the KRAKEN platform.[243] Natural persons can either operate in their own name or on behalf of a company. In case of the latter, it must have been authorized by a legal representative of the company and the company must have been object of an identification process by KRAKEN. [244] For authentication KRAKEN makes use of SSI. The user registration process is implemented by issuing a MarketplaceRegistration VC from the Marketplace to the user, which will be presented as proof by the user to the Marketplace on subsequent access.[245] The MarketplaceRegistration VC avoids storing the user's data in the Marketplace repository, instead the data will be saved on the VC and stored in the user SSI wallet in full control of the user.[246]	
Outline of the processing under consideration		
What are the data processed?	• First name; • last name; • e-mail address; • country of residence; • age (i.e., 18 years or older in compliance with data minimization requirements). In addition to the above, if the user is a natural person representing an organization/institution: • name of organization / institution; • type of organization / institution; • name of the legal representative of the organization;	All this information is necessary for the operation of the marketplace, except for invoicing details, which are only required if an organizational/institutional user prefers to receive fiat currencies over cryptocurrencies. The name of the organization, type of organization, name of the legal representative of the organization, and Data Protection Officer's email address are only obligatory fields of information for organizational/institutional users.

[243] KRAKEN D5.4 'Final KRAKEN marketplace integrated architecture', 13.

[244] Ibid., 13.

[245] KRAKEN D2.3 'Final KRAKEN architecture', 15.

[246] Ibid., 15.

Question	Answer	Comments
	• Data Protection Officer's email address; • invoicing details for fiat payments; and • decentralized Identifier (DID) connection identity (ID) used on the first time they connect with the marketplace.[247]	
Identify data controller and any processors	KRAKEN is the sole controller in relation to account data.	KRAKEN determines the means and purposes of processing of account data.
Purpose of the processing	To create and maintain a KRAKEN user account and make use of the KRAKEN platform service. It may also be necessary to comply with a legal obligation for the purpose of legal compliance, tax or auditing purposes, or to detect and prevent fraudulent or illegal activity.	KRAKEN must be able to uniquely identify the user in order to provide the KRAKEN platform service. KRAKEN must also be able to comply with legal obligations in relation to account data.
Compliance with fundamental principles		
Are the processing purposes specified, explicit and legitimate?	Yes	The processing purposes are explicitly and clearly stated in the KRAKEN Privacy Policy. They are necessary and sufficiently specific to achieve the goals of the KRAKEN platform. Furthermore, the purposes are legitimate and not unlawful in any way.
Legal basis of the processing?	KRAKEN relies on two legal bases for the processing of account data.	Account data is processed based on the necessity for the performance of a contract. It may also be the case that KRAKEN processes account data based on a legal obligation.
Adequate, relevant and limited to what is necessary in relation to the purposes for	Yes	Account data are necessary for the performance of the contract between KRAKEN and the user, which exists in the creation and

[247] KRAKEN D2.7 'Design for marketplace reference implementations', 15.

Question	Answer	Comments
which they are processed ('data minimisation')?		maintenance of a KRAKEN user account and the subsequent usage of the KRAKEN platform service. Account data may also be necessary for the compliance with a legal obligation (e.g., legal compliance, tax or auditing purposes, or to detect and prevent fraudulent or illegal activity). Account data has been limited to what is necessary for the specified purposes (e.g., 18 years or older instead of a specific birthdate).
Accurate and kept up to date?	Self-provided by the user.	Data subjects are able to rectify their account data through the KRAKEN user profile or by contacting KRAKEN.
Storage duration of the data?	The extent and period of processing (incl. storage) of account data are limited to what is strictly necessary for the processing purposes.	Data subjects are able to obtain the erasure of their account data by deleting their KRAKEN user account through the KRAKEN user profile or by contacting KRAKEN. As the information is kept on the MarketplaceRegistration VC which is under control of the user, the user can decide themselves how long the data should be made available. No personal data of the user is stored on the blockchain.
Data subject rights		
How are the data subjects informed?	Via the KRAKEN Privacy Policy and disclaimers throughout the KRAKEN account registration process.	The KRAKEN Privacy Policy includes clear and intelligible information on the processing of account data.
How is the consent obtained and how can it be withdrawn?	N/A: the processing of account data is not based on consent, but rather on the necessity for the performance of a contract.	

Question	Answer	Comments
How can data subjects exercise their rights of access and to data portability?	Data subjects may contact KRAKEN to exercise their rights as a data subject in relation to account data. Information on how to exercise data subject rights and relevant contact details may be found in the KRAKEN Privacy Policy.	The data subject has the MarketplaceRegistration VC in its wallet and can in principle use it to transfer the data also to somewhere else.
How can data subjects exercise their rights to rectification and erasure?	Data subjects are able to rectify their account data through the KRAKEN user profile or by contacting KRAKEN. Data subjects are able to obtain the erasure of their account data by deleting their KRAKEN user account through the KRAKEN user profile or by contacting KRAKEN.	As the information is kept on the MarketplaceRegistration VC which is under control of the user, the user can decide themselves how long the data should be made available. No personal data of the user is stored on the blockchain.
How can data subjects exercise their rights to restriction and to object?	By contacting KRAKEN, data subjects are able to object at any time to the processing of their account data for direct marketing purposes, which includes profiling to the extent that it is related to such direct marketing. Data subjects are able to contact KRAKEN to obtain the restriction of processing of account data under certain conditions.	Data subjects may also indirectly object to the processing of their account data by exercising their right to erasure (by deleting their KRAKEN user account through the KRAKEN user profile or by contacting KRAKEN).
Are the obligations of the processors clearly identified and governed by a contract?	N/A: there are no other parties that act as processors in relation to account data.	
In the case of data transfer outside the European Union, are the data adequately protected?	N/A: KRAKEN does not transfer account data to third countries or international organizations.	The use of distributed ledger technology does not involve the storage of account on nodes outside of the EEA.

Planned or existing measures
The MarketplaceRegistration VC avoids storing the user's personal data in the Marketplace repository.

Question	Answer	Comments
This data will be saved in the MarketplaceRegistration VC and stored in the user SSI wallet in the full control of the user. They will be required by the Marketplace as an SSI proof[248] when the user logs in to the Marketplace.[249]		
The KRAKEN Privacy Policy informs users and data subjects in a clear and intelligible manner about the processing activities and purposes relating to account data.		
Data subjects may contact KRAKEN to exercise their rights as a data subject in relation to account data. Information on how to exercise data subject rights and relevant contact details may be found in the KRAKEN Privacy Policy.		
The GDPR's requirement of the right to be forgotten will be implemented under the full control of the user. When the user decides to be forgotten by the Marketplace, one of the actions that the Marketplace will perform is the revocation of the MarketplaceRegistration VC, invalidating it for future usage and in a way that is evident to the user that has the VC inside her/his wallet.[250]		
Risk		
Illegitimate access to personal data (i.e., confidentiality)		
What could be the main impacts on the data subjects if the risk were to occur?	Unauthorized access to account data could result in the identification of KRAKEN users. Although the impact would be low considering the limited potential harm of identification, small scale of processing, and non-sensitive nature of the data, this information could be used for malicious purposes.	
What are the main threats that could lead to the risk?	A vulnerability in the security of the KRAKEN platform and the unauthorized access to account data.	
What are the risk sources?	Actors aiming to obtain personal data of users.	
Which of the identified controls contribute to addressing the risk?	The implementation of end-to-end encryption, strong web security, and access policies aim at protecting the confidentiality of data in transit and at rest.	
How do you estimate the risk severity, especially according to potential impacts and planned controls?	The overall severity of the risk is low considering the low impact and low likelihood.	
How do you estimate the likelihood of the risk, especially in respect of threats, sources of risk and planned controls?	The likelihood of the risk is low. It is unlikely that an actor would obtain unauthorized access to account data considering the small scale of processing, non-sensitive nature of the data, and implemented authorization measures.	
What else could potentially be done to minimise the risk?	The risk is already low and there are technical and organizational measures in place to protect the confidentiality of account data.	

[248] KRAKEN D2.3 'Final KRAKEN architecture', 15.

[249] Ibid., 15.

[250] Ibid., 15.

Question	Answer	Comments
	More stringent security measures could potentially further minimise the risk (e.g., more stringent authorization measures, limiting authorized personnel, etc.).	
Unwanted change of personal data (i.e., integrity)		
What could be the main impacts on the data subjects if the risk were to occur?	The unwanted change of account data could result in inaccurate account data and potentially impair transactions on the KRAKEN platform (e.g., country of residence affects applicable national data protection provisions). Although the impact would be low considering the limited potential harm, actors could change account data for malicious purposes.	
What are the main threats that could lead to the risk?	A vulnerability in the security of the KRAKEN platform and the unauthorized access account data.	
What are the risk sources?	Actors aiming to change the account data of users.	
Which of the identified controls contribute to addressing the risk?	KRAKEN users are able to rectify account data through the KRAKEN profile or by contacting KRAKEN. KRAKEN also has the ability to rectify account data that has been changed. The implementation of strong web security also aims at protecting the integrity of data.	
How do you estimate the risk severity, especially according to potential impacts and planned controls?	The overall severity of the risk is low considering the low impact and low likelihood.	
How do you estimate the likelihood of the risk, especially in respect of threats, sources of risk and planned controls?	The likelihood of the risk is low. It is unlikely that an actor would make changes to account data considering the limited potential harm.	
What else could potentially be done to minimise the risk?	The risk is already low and there are technical measures in place to protect the integrity of account data. More stringent security measures could potentially further minimise the risk (e.g., additional authorization measures, write and modification permissions, additional protection against external influences, periodic security assessments, etc.).	
Disappearance of personal data (i.e., availability)		
What could be the main impacts on the data subjects if the risk were to occur?	In case account data is not available or access is not possible, this could result in the impairment of transactions on the KRAKEN platform. The impact would be low considering the limited potential harm for the rights and freedoms of data subjects.	
What are the main threats that could lead to the risk?	A vulnerability in the security of the KRAKEN platform.	
What are the risk sources?	Actors aiming to erase or disable access to account data.	

Question	Answer	Comments
	The accidental erasure of account data by KRAKEN.	
Which of the identified controls contribute to addressing the risk?	KRAKEN users are able to provide account data to KRAKEN in order to restore lost data. KRAKEN is able to restore account data in case of non-availability.	
How do you estimate the risk severity, especially according to potential impacts and planned controls?	The overall severity of the risk is low considering the low impact and low likelihood.	
How do you estimate the likelihood of the risk, especially in respect of threats, sources of risk and planned controls?	The likelihood of the risk is low. It is unlikely that an actor would erase or disable access to account data considering the limited potential harm.	
What else could potentially be done to minimise the risk?	The risk is already low and there are technical and organizational measures in place to protect the availability of account data. More stringent security measures could potentially further minimise the risk (e.g., backups, additional measures against external influences, repair strategies, contingency plans, etc.).	
Unlinkability		
What is done to support this data protection goal?	Account data are collected for the same purposes. The amount of account data is limited and the scale of processing activities is small. The use of technical (e.g., end-to-end encryption) and organizational measures (e.g., access policies) further support unlinkability.	
What could be the main impacts on the data subjects if the data were linkable?	Since account data includes the first and last name of users, data subjects are already identifiable by creating a KRAKEN account. An external actor could therefore also identify KRAKEN users by linking account data together. The impact on data subjects would be low considering the limited amount of account data and limited potential harm of identification.	
What are the main threats that could lead to the risk?	A vulnerability in the security of the KRAKEN platform.	
What are the risk sources?	Actors aiming to link account data together.	
Which of the identified controls contribute to addressing the risk?	Collection of account data for specified purposes, a limited amount of account data, and small scale of processing activities. The use of technical (e.g., end-to-end encryption) and organizational measures (e.g., access policies) further support unlinkability.	
How do you estimate the risk severity, especially according	The overall severity of the risk is low considering the low impact and low likelihood.	

Question	Answer	Comments
to potential impacts and planned controls?		
How do you estimate the likelihood of the risk, especially in respect of threats, sources of risk and planned controls?	The likelihood of the risk is low. It is unlikely that an actor would make efforts to link account data together considering the limited potential harm of identification.	
What else could potentially be done to minimise the risk?	The risk is already low and there are technical and organizational measures in place to protect the unlinkability of data. More stringent security measures could potentially further minimise the risk (e.g., additional measures against external influences, restrictions of permissions for processing, etc.).	
Transparency		
What is done to support this data protection goal?	The KRAKEN platform implements a user-friendly interface with additional information notices on the rights and obligations under the GDPR. The KRAKEN Privacy Policy further describes the processing activities, purposes, legal bases, and data subject rights in a concise, transparent, intelligible and easily accessible form, using clear and plain language. Data subjects are able to contact KRAKEN in case they require additional information. KRAKEN also provides privacy metrics which further inform users about their level of privacy.	
What could be the main impacts on the data subjects if the processing would not be transparent?	Data subject would not be properly informed about the processing activities relating to account data as well as their rights and freedoms under the GDPR. The impact would be medium considering the effect on the rights and freedoms of data subjects.	
What are the main threats that could lead to the risk?	Insufficient or unclear information on processing activities, purposes, legal bases, and data subject rights.	
What are the risk sources?	Incomplete or unclear information notices and Privacy Policy.	
Which of the identified controls contribute to addressing the risk?	Providing information relating to processing in a concise, transparent, intelligible and easily accessible form, using clear and plain language.	
How do you estimate the risk severity, especially according to potential impacts and planned controls?	The overall severity of the risk is low considering the medium impact and low likelihood.	
How do you estimate the likelihood of the risk, especially in respect of threats,	The likelihood of the risk is low considering the necessary information has been provided in a transparent manner.	

Question	Answer	Comments
sources of risk and planned controls?		
What else could potentially be done to minimise the risk?	The risk is already low. However, further refining and expanding on the provided information could improve transparency.	
Intervenability		
What is done to support this data protection goal?	The KRAKEN Privacy Policy informs data subjects about their rights and how to exercise them. KRAKEN is able to act without undue with regard to requests to exercise data subject rights. KRAKEN is also able to take measures in relation to data processing, such as the erasure of account data.	
What could be the main impacts on the data subjects if it was not possible to intervene?	Data subject would not be properly informed about their rights and freedoms under the GDPR. This would also impair their ability to effectively exercise their data subject rights. The impact would be medium considering the effect on the rights and freedoms of data subjects.	
What are the main threats that could lead to the risk?	Insufficient or unclear information on data subject rights. The lack of measures enabling KRAKEN to act upon requests to exercise data subject rights.	
What are the risk sources?	Incomplete or unclear information notices and Privacy Policy. Technical obstacles regarding the exercise of data subject rights.	
Which of the identified controls contribute to addressing the risk?	Providing information relating to data subject rights in a concise, transparent, intelligible and easily accessible form, using clear and plain language. The ability of KRAKEN to act upon requests to exercise data subject rights or take measures in relation to data processing.	
How do you estimate the risk severity, especially according to potential impacts and planned controls?	The overall severity of the risk is low considering the medium impact and low likelihood.	
How do you estimate the likelihood of the risk, especially in respect of threats, sources of risk and planned controls?	The likelihood of the risk is low considering the necessary information has been provided in a transparent manner and KRAKEN is able to act upon requests.	
What else could potentially be done to minimise the risk?	The risk is already low. However, further improving the technical and organizational capabilities to act upon requests could further minimise the risk (e.g., dedicated interface for the exercise of data subject rights, etc.).	

Table 5: DPIA table account data

DPIA table batch data

Question	Answer	Comments
Context		
What is the processing under consideration?	The processing under consideration is the provision and consumption of batch data (static record or collection of files).[251] The user can be a controller providing data (e.g., anonymous data or data for which a valid consent has been provided to share it via KRAKEN with specific data consumers for specific purposes), or a data subject which wants to share own personal data via KRAKEN. The user encrypts the dataset using the web page provided by the Marketplace. This process does not send any data to the KRAKEN Marketplace servers, it just encrypts the dataset and gives it back to the user.[252] The user uploads the encrypted dataset on his own cloud storage and then fills all the required fields for the Data Product publication such as title, description, image, tags, the policies that will govern the access to the Data Product, cloud storage link and the price. [253] The information is submitted to the Marketplace API. [254] Part of the info provided to the API, including price, is sent to the Marketplace smart contract running on the xDai network to enable payments on the Data Product. [255] The permissioning blockchain is updated with the new Data Product and its policies.[256] The SMPC network is updated with the new Data Product and the encryption key shares (a set of information that will let the data consumers access the dataset without giving the marketplace access to the decryption key).[257]	
Outline of the processing under consideration		
What are the data processed?	Related to batch data: • encryption of batch data; • location batch data on cloud server; and • metadata of batch data: e.g., data product policies, who bought access to the data. Batch data itself:	When a data provider using the Marketplace Frontend publishes a Data Product, the Marketplace Frontend sends the Data Product's associated metadata to the Marketplace Backend API. This includes the Data Product's descriptive information, policies and cloud storage link. The Marketplace Backend stores this information and also sends the

[251] KRAKEN D2.7 'Design for marketplace reference implementations', 10.
[252] KRAKEN D2.3 'Final KRAKEN architecture', 20.
[253] Ibid., 20.
[254] Ibid., 20.
[255] Ibid., 20.
[256] Ibid., 20.
[257] Ibid., 20.

Question	Answer	Comments
	• processing of batch data by data consumer.	Data Products policies to be recorded on the Lynkeus blockchain.[258] The data provider provides the information whether the batch data includes personal data and sensitive personal data. Recommendation: it would be useful to add an explanation to guide the data provider so that he will indicate the correct information.
Identify data controller and any processors	Related to batch data: KRAKEN platform owner. Batch data itself: Data consumer. Data provider, if not data subject.	It is assumed that the KRAKEN platform will not be a controller regarding the batch data. It might be a controller for the encryption of the data, as this constitutes processing of personal data. For the batch data, the data consumer will be the receiving controller, while the data provider will be a controller, if it provides data from other data subjects.
Purpose of the processing	Related to batch data: • encryption of batch data: to keep the data secure; and • metadata/location of cloud storage: to provide the service. Batch data itself: Depends on the purpose of the data consumer, must be within the allowed purpose of the data provider.	When providing the data and when buying access to the data, the user interface requires to select purposes, and allows only access to the data when the purposes match. The selection of purposes is at the moment: Marketing, management or improvement of business services, publicly funded research, private research and automated decision-making, e.g., Artificial intelligence (including profiling).
Compliance with fundamental principles		
Are the processing purposes specified, explicit and legitimate?	Related to batch data: • encryption of batch data;	Purpose options are rather general, to add an open field would be better.

[258] KRAKEN D5.4 'Final KRAKEN marketplace integrated architecture', 19.

Question	Answer	Comments
	• processing of metadata and location of cloud storage; and • purpose: to provide the service to the data provider. Batch data itself: The selection of purposes is at the moment: Marketing, management or improvement of business services, publicly funded research, private research and automated decision-making, e.g., Artificial intelligence (including profiling).	
Legal basis of the processing?	Related to batch data: Encryption: consent. Processing of metadata and location of cloud storage: necessary for a contract. Batch data itself: Consent of the data subject.	Batch data: danger that the providing controller shares data for which no valid consent had been obtained.
Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')?	Related to batch data: • metadata; and • encryption: limited to what is necessary, will encrypt data and user can download it, system does not keep it. Batch data itself: Depends on what data will be provided and consumed. Data will not be copied/stored at the KRAKEN system.	
Accurate and kept up to date?	Related to batch data: The encrypted data will not be stored by KRAKEN but given to the data provider to store. Batch data itself: Provider as data subject: can keep it up to date themselves.	

Question	Answer	Comments
	Provider as controller: own responsibility. Consumer: own responsibility.	
Storage duration of the data?	Related to batch data: The encrypted data will not be stored by KRAKEN but given to the data provider to store. Batch data itself: On provider side, the data provider can decide themselves how long they will make it available. They can specify how long it may be stored, they can delete it from the cloud storage and they can request deletion via the dashboard. On consumer side, the data consumer must provide information on how long the data will be stored.	Metadata is stored until a user deletes the related data product. By deleting a data product in the marketplace, metadata is removed from the marketplace Backend database and marketplace Frontend catalogue. No product metadata is stored on the blockchain, only permissions. Potential issue whether the data consumer will indeed delete the data within the specified time-frame. KRAKEN provides a message to the data consumer to make clear the data must be deleted and processing activities must cease after the specified time-frame.
Data subject rights		
How are the data subjects informed?	Related to batch data: The information should be included in the privacy policy. Batch data itself: Data subjects normally know which data will be processed, as they provide the data themselves and chose the options for processing. Furthermore, they are informed through the privacy policy and disclaimers throughout the registration and publication processes and will get specific information on the data consumer, after the data consumer buys access to the data. This information will be available through the dashboard. In case the data provider is a controller, it is the data	

Question	Answer	Comments
	providers obligation to inform the data subjects.	
How is the consent obtained and how can it be withdrawn?	Related to batch data: Via the provision of the information. Can be withdrawn by deleting the information. Batch data itself: The data subject gives proactively consent within certain parameters. It can easily withdraw consent in marketplace mobile app.	Consent if data provider is controller: outside of scope of KRAKEN; cannot be verified. Withdrawal of consent: through the marketplace mobile app or e-mail to data consumer to delete the data; cannot be verified. Could potentially use contractual obligations.
How can data subjects exercise their rights of access and to data portability?	Related to batch data: The data subject gets the encrypted data immediately after encryption. Can access the metadata. Batch data itself: Via the contact details of the data consumer, provided in the dashboard.	Batch data: Outside of KRAKEN, no possibility to ensure compliance of the data consumer. Could potentially use contractual obligations.
How can data subjects exercise their rights to rectification and erasure?	Related to batch data: DS gets the encrypted data immediately after encryption. Batch data itself: Via the contact details of the data consumer, provided in the dashboard.	Batch data: Outside of KRAKEN, no possibility to ensure compliance of the data consumer. Could potentially use contractual obligations.
How can data subjects exercise their rights to restriction and to object?	Related to batch data: DS gets the encrypted data immediately after encryption. Batch data itself: Via the contact details of the data consumer, provided in the dashboard.	Batch data: Outside of KRAKEN, no possibility to ensure compliance of the data consumer. Could potentially use contractual obligations.
Are the obligations of the processors clearly identified and governed by a contract?	N/A	N/A

Question	Answer	Comments
In the case of data transfer outside the European Union, are the data adequately protected?	Related to batch data: No data transfer. Batch data itself: Data transfer possible, depending on what the data provider indicates.	Outside of KRAKEN, no possibility to ensure compliance of the data consumer. Could potentially use contractual obligations.
Planned or existing measures		
Eligibility of buyers checked by Lynkeus blockchain.[259]		
Data protection layer: secure multi party computation system for encryption keys sharing mechanism[260]: The secure sharing of datasets for batch datasets is enforced by the encryption performed on the marketplace and the key exchange performed by the SMPC network. The data is encrypted and stored on a cloud storage managed by the data provider.[261]		
Encryption at rest and transaction.[262]		
Data provenance parameter to track the entire life cycle of a data product, including aggregated forms of the product derived from Data Unions or other data mergers?[263]		
Dynamic consent.		
Dashboard to easily exercise the data subject rights.		
Privacy metrics.		
Risk: (batch data itself)		
Illegitimate access to personal data (-> confidentiality)		
What could be the main impacts on the data subjects if the risk were to occur?	That data that the data provider only wanted to make accessible to certain data consumers becomes accessible to other persons. The impact depends entirely upon the type of data.	
What are the main threats that could lead to the risk?	• Access via the cloud storage, breach of encryption; • data consumer who is not eligible gets access to storage location and keys; • access to data during encryption process; and • data consumer does not keep the data secure/shares it with another entity.	
What are the risk sources?	• Adversary; • data consumer; and • failure in the KRAKEN system/smart contracts giving access.	

[259] KRAKEN D2.7 'Design for marketplace reference implementations', 16.
[260] KRAKEN D5.4 'Final KRAKEN marketplace integrated architecture', 10.
[261] KRAKEN D2.7 'Design for marketplace reference implementations', 16.
[262] KRAKEN D5.4 'Final KRAKEN marketplace integrated architecture', 10.
[263] Ibid., 11.

Question	Answer	Comments
Which of the identified controls contribute to addressing the risk?	• SSI login; • eligibility of buyers checked by Lynkeus blockchain; and • secure multi party computation system for encryption keys sharing mechanism.	
How do you estimate the risk severity, especially according to potential impacts and planned controls?	Depends on the type of data.	
How do you estimate the likelihood of the risk, especially in respect of threats, sources of risk and planned controls?	Depends on the type of data.	
What else could potentially be done to minimise the risk?		
Unwanted change of personal data (-> integrity)		
What could be the main impacts on the data subjects if the risk were to occur?	It depends on the type of data that is shared.	
What are the main threats that could lead to the risk?	• Changes at the cloud storage; • changes at the data consumer; and • something going wrong with the encryption.	
What are the risk sources?	• Cloud provider; • data consumer; • data subject; and • technical failure during encryption.	
Which of the identified controls contribute to addressing the risk?	• Encryption; • the data is not stored at KRAKEN; and • data provenance.	
How do you estimate the risk severity, especially according to potential impacts and planned controls?	Depends on the type of data.	
How do you estimate the likelihood of the risk, especially in respect of threats, sources of risk and planned controls?	Depends on the type of data.	
What else could potentially be done to minimise the risk?		

Question	Answer	Comments
Disappearance of personal data (-> availability)		
What could be the main impacts on the data subjects if the risk were to occur?	Impact could be that they do not get the money for access to the data if it is not there.	
What are the main threats that could lead to the risk?	• Cloud failure; and • fault of the data subject.	
What are the risk sources?	• Cloud provider; and • data subject.	
Which of the identified controls contribute to addressing the risk?	Outside of the scope of KRAKEN.	
How do you estimate the risk severity, especially according to potential impacts and planned controls?	Low	
How do you estimate the likelihood of the risk, especially in respect of threats, sources of risk and planned controls?	Low, assuming that the data subject does have a backup of the data.	
What else could potentially be done to minimise the risk?	Inform the data subject to keep a backup since KRAKEN does not store the information.	
Unlinkability		
What is done to support this data protection goal?	Option to use data analytics. Privacy metrics.	
What could be the main impacts on the data subjects if the data were linkable?	Depends on the data.	
What are the main threats that could lead to the risk?	Data consumer/adversary obtains data and links it to obtain more information about the data subject.	
What are the risk sources?	• Data consumer; and • adversary.	
Which of the identified controls contribute to addressing the risk?	• Data analytics; • privacy metrics; and • data provenance.	
How do you estimate the risk severity, especially according to potential impacts and planned controls?	Depends upon the type of data.	

Question	Answer	Comments
How do you estimate the likelihood of the risk, especially in respect of threats, sources of risk and planned controls?	Depends upon the type of data.	
What else could potentially be done to minimise the risk?	Promote the use of data analytics and the use of privacy metrics.	
Transparency		
What is done to support this data protection goal?	Dashboard. Information in user interface. Selection of criteria by data provider.	
What could be the main impacts on the data subjects if the processing would not be transparent?	Misunderstand the scope and protection of KRAKEN, put more trust in it than reasonable. False information from the data consumer.	
What are the main threats that could lead to the risk?	Insufficient/unclear /false information.	
What are the risk sources?	• KRAKEN platform; and • data consumer.	
Which of the identified controls contribute to addressing the risk?	All that help to give more information to the data subject: information in user interface, dashboard, privacy policy etc.	
How do you estimate the risk severity, especially according to potential impacts and planned controls?	In principle low.	
How do you estimate the likelihood of the risk, especially in respect of threats, sources of risk and planned controls?	In principle low.	
What else could potentially be done to minimise the risk?	The marketing should be cautious not to create wrong expectations for the system.	
Intervenability		
What is done to support this data protection goal?	• Dashboard; • dynamic consent; and • information to the data consumer that they need to comply with data subjects rights requests/withdrawal of consent.	
What could be the main impacts on the data subjects if	Loss of trust in the system. Depends on the data.	

Question	Answer	Comments
it was not possible to intervene?		
What are the main threats that could lead to the risk?	Non-complying data consumer.	
What are the risk sources?	Data consumer.	
Which of the identified controls contribute to addressing the risk?	• Dashboard; • dynamic consent; and • storage of the data at the data provider premises (can delete it/change it).	
How do you estimate the risk severity, especially according to potential impacts and planned controls?	Depends upon the data.	
How do you estimate the likelihood of the risk, especially in respect of threats, sources of risk and planned controls?	Depends upon the data.	
What else could potentially be done to minimise the risk?	Clear information to the data consumer that they need to comply with data subject rights requests/withdrawal of consent, contractual obligations.	

Table 6: DPIA table batch data

DPIA table data analytics

Question	Answer	Comments
Context		
What is the processing under consideration?	The processing under consideration is the provision of Data analytics: the provision of computations of functions on the data with secure multi party computation (SMPC). The data provider can indicate that the data might be also or exclusively used for data analytics. Data provider splits data into shares and uploads them in an encrypted form that can be accessed only by the SMPC nodes. [264] KRAKEN Frontend provides a functionality that allows a user to load the dataset (locally) in his/her web browser, during the process of publication, and then split and encrypt the dataset using public keys of the SMPC nodes. [265] This is implemented using WebAssembly that allows running complex programs (in our case implemented in Go) directly in a browser. [266] Marketplace's Backend receives only a link to the location of the encrypted data that it cannot access.[267] Data is split into shares, such that without knowing enough of them, no information about the data can be revealed. [268] The shares are distributed among SMPC nodes (servers participating in SMPC network), so that they can interactively compute a function on the data without knowing the data or the result themselves. [269] The (shares of) results are delivered to a buyer of a computation, who can merge hem in the final result.[270] On receiving requests from users to perform analytics computations on the data via the Marketplace Frontend, the Marketplace Backend API checks with the Lynkeus Blockchain that the consumers are eligible.[271] If the data consumer is confirmed as eligible they are able to use the Marketplace Frontend to process a payment to the data provider using the Streamr DATA token on the xDai blockchain. [272] If the payment has been successfully transferred to the corresponding Data Product owners, a notification is sent to the Marketplace Backend API by the xDai blockchain that confirms the payment.[273] Upon receipt of the payment notification from the xDai blockchain, the Marketplace Backend API communicates with the integrated SMPC Network to trigger the download of the encrypted secret	

[264] Ibid., 18.
[265] Ibid., 18.
[266] Ibid., 18.
[267] Ibid., 18.
[268] Ibid., 17.
[269] Ibid., 17.
[270] Ibid., 17.
[271] Ibid., 19.
[272] Ibid., 19.
[273] Ibid., 19.

Question	Answer	Comments
	shares from the data providers' cloud storage.[274] This could be data from a single data provider or Data Product, or it could be data from multiple data providers or Data Products.[275] The SMPC Network finally computes the analytics and returns the results to the Marketplace Backend API.[276] These results are encrypted specifically for the user requesting the analytics.[277] Once the results are received by the Marketplace Backend API, the user requesting the analytics then uses the Marketplace Frontend to download and decrypt the results in a CSV file format.[278] For data that is available for privacy-preserving analytics via SMPC, a data consumer will be able to use the marketplace GUI to purchase computation packages that are tiered in gold, silver and bronze packages. Once purchased they will trigger the query of pre-defined privacy-preserving analytics.[279] It is not anticipated that detailed permissions about the purposes of use will be required for privacy-preserving analytics as no personal data will be shared with the data users in this modality.[280]	
Outline of the processing under consideration		
What are the data processed?	Depends on the content data provided by the data provider. Processing by KRAKEN: splitting & encryption of data and location of encrypted data.	
Identify data controller and any processors	Marketplace acts as intermediary between data provider and data consumer. Content data are never stored by the marketplace. Marketplace provider of analytics function: processor or controller, joint with data consumer. SMPC nodes: processor/sub-processor.	It is assumed that KRAKEN will act as a processor for the data consumer, as the processing only occurs upon request and for the purposes defined by the data consumer. The SMPC nodes will be considered sub-processors.
Purpose of the processing	Doing the analytics. Making the analytics possible in a privacy respecting manner	

[274] Ibid., 19.
[275] Ibid., 19.
[276] Ibid., 19.
[277] Ibid., 19.
[278] Ibid., 19.
[279] KRAKEN D2.7 'Design for marketplace reference implementations', 47.
[280] Ibid., 47.

Question	Answer	Comments
	(splitting and encrypting the data).	
Compliance with fundamental principles		
Are the processing purposes specified, explicit and legitimate?	Yes	
Legal basis of the processing?	Consent for analytics.	
adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')?	Yes	
Accurate and kept up to date?	Will be obtained from the store of the data provider.	
Storage duration of the data?	The nodes delete the data after the analysis.	
Data subject rights		
How are the data subjects informed?	The data provider can see who accessed the data in the dashboard.	
How is the consent obtained and how can it be withdrawn?	Via providing the data for data analytics going through the entire process and UI in order to employ analytics.	
How can data subjects exercise their rights of access and to data portability?	As the data shares are immediately deleted after the analysis, and the result of the analysis is supposed to be anonymous, it is not possible to exercise data subject rights after the analysis.	
How can data subjects exercise their rights to rectification and erasure?	As the data shares are immediately deleted after the analysis, and the result of the analysis is supposed to be anonymous, it is not possible to exercise data subject rights after the analysis.	
How can data subjects exercise their rights to restriction and to object?	As the data shares are immediately deleted after the analysis, and the result of the analysis is supposed to be anonymous, it is not possible to	

Question	Answer	Comments
	exercise data subject rights after the analysis.	
Are the obligations of the processors clearly identified and governed by a contract?	A contract between KRAKEN and the nodes would be necessary.	
In the case of data transfer outside the European Union, are the data adequately protected?	Nodes will be within the EU.	
Planned or existing measures		
Encryption		
Requests are recorded and checked by the SMPC nodes on a KRAKEN blockchain preventing privacy violating behaviour.[281]		
A data provider who is concerned about the security and privacy of their data assets can create a Data Product that is only available for analytics, and receive payment in the form of the Streamr DATA token every time a data user performs a computation that involves their Data Product.[282]		
A Data Product's secret shares can only be downloaded by the nodes in the SMPC network for computing the analytics on behalf of the data user after two important steps have been verified by the marketplace: 1) a user who wants to perform analytics has been confirmed as eligible to access the Data Product by the Lynkeus blockchain; and 2) a payment notification has been received by the Marketplace from the xDai blockchain.[283]		
Dynamic consent.		
Nodes are located in the EU.[284]		
Data providers able to monitor/manage privacy budgets?[285]		
Risk		
Illegitimate access to personal data (-> confidentiality)		
What could be the main impacts on the data subjects if the risk were to occur?	That data that they only wanted to make accessible via data analytics is accessible. The impact depends entirely upon the type of data.	
What are the main threats that could lead to the risk?	• Failure of SMPC/system (provides access as batch data instead of data analytics); and • not enough data points so that the analytics basically give the data as result.	
What are the risk sources?	• KRAKEN; and • adversaries breaking the SMPC.	

[281] KRAKEN D5.4 'Final KRAKEN marketplace integrated architecture', 18.

[282] Ibid., 19.

[283] Ibid., 19.

[284] KRAKEN D2.7 'Design for marketplace reference implementations', 24.

[285] Ibid., 27.

Question	Answer	Comments
Which of the identified controls contribute to addressing the risk?	The whole system is aimed at providing confidentiality for the data.	
How do you estimate the risk severity, especially according to potential impacts and planned controls?	Depends upon the type of data.	
How do you estimate the likelihood of the risk, especially in respect of threats, sources of risk and planned controls?	As the whole aim of the system is to ensure confidentiality, while it is not expected that the data will attract highly skilled adversaries breaking the SMPC, the risk is considered rather low.	
What else could potentially be done to minimise the risk?	Ensure that the data analytics function works as required.	
Unwanted change of personal data (-> integrity)		
What could be the main impacts on the data subjects if the risk were to occur?	Failure in the analytics could lead to wrong processes if decisions are taken based on the analytics results.	
What are the main threats that could lead to the risk?	Wrong naming of the columns, etc.	
What are the risk sources?	• Data subject; and • KRAKEN.	
Which of the identified controls contribute to addressing the risk?		
How do you estimate the risk severity, especially according to potential impacts and planned controls?	Low	
How do you estimate the likelihood of the risk, especially in respect of threats, sources of risk and planned controls?	Failed analyses might happen, but it is unlikely that it will result in impacts upon the data subject or other natural persons, since it is unlikely that decisions will be based entirely on data that cannot be verified by the researchers.	
What else could potentially be done to minimise the risk?	Provide guidance how to prepare the data for analytics.	
Disappearance of personal data (-> availability)		
What could be the main impacts on the data subjects if the risk were to occur?	Do not get money for access to the data if data is not there.	

Question	Answer	Comments
What are the main threats that could lead to the risk?	The encrypted data shares are lost.	
What are the risk sources?	KRAKEN	
Which of the identified controls contribute to addressing the risk?		
How do you estimate the risk severity, especially according to potential impacts and planned controls?	Low	
How do you estimate the likelihood of the risk, especially in respect of threats, sources of risk and planned controls?	Low	
What else could potentially be done to minimise the risk?	Regularly test the system.	
Unlinkability		
What is done to support this data protection goal?	• Data analytics themselves are a measure to provide unlinkability of the data; and • privacy metrics.	
What could be the main impacts on the data subjects if the data were linkable?	Depends on the data.	
What are the main threats that could lead to the risk?	• Not sufficient data to provide unlinkability via data analytics; and • possibility to link different data sets after data analytics due to additional knowledge.	
What are the risk sources?	• Data subject not providing enough data; • adversary able to link the data; and • data consumer able to link the data.	
Which of the identified controls contribute to addressing the risk?	Privacy metrics.	
How do you estimate the risk severity, especially according to potential impacts and planned controls?	Depends upon the type of data.	
How do you estimate the likelihood of the risk, especially in respect of threats,	Depends upon the type of data.	

Question	Answer	Comments
sources of risk and planned controls?		
What else could potentially be done to minimise the risk?	Controls to ensure that the result of the analysis is anonymous/unlinkable.	
Transparency		
What is done to support this data protection goal?	• Dashboard; • information in user interface; and • selection of criteria by data provider.	
What could be the main impacts on the data subjects if the processing would not be transparent?	Misunderstand the scope and protection of KRAKEN, put more trust in it than reasonable. False information from the data consumer.	
What are the main threats that could lead to the risk?	Insufficient/unclear /false information.	
What are the risk sources?	• KRAKEN platform; and • data consumer.	
Which of the identified controls contribute to addressing the risk?	• Dashboard; • information in user interface; and • selection of criteria by data provider.	
How do you estimate the risk severity, especially according to potential impacts and planned controls?	Low	
How do you estimate the likelihood of the risk, especially in respect of threats, sources of risk and planned controls?	Low	
What else could potentially be done to minimise the risk?	More information provided to explain how the system works and what can be expected.	
Intervenability		
What is done to support this data protection goal?	• Dashboard; and • dynamic consent.	
What could be the main impacts on the data subjects if it was not possible to intervene?	Loss of trust in the system. Depends on the data.	
What are the main threats that could lead to the risk?	Non-complying data consumer.	
What are the risk sources?	Data consumer.	

Question	Answer	Comments
Which of the identified controls contribute to addressing the risk?	• Dashboard; • dynamic consent; and • storage of the data at the data provider premises (can delete it/change it).	
How do you estimate the risk severity, especially according to potential impacts and planned controls?	Depends upon the data, but rather low, since normally the data will be statistics and anonymous, so no intervenability necessary.	
How do you estimate the likelihood of the risk, especially in respect of threats, sources of risk and planned controls?	Rather low, since normally the data will be statistics and anonymous, so no intervenability necessary.	
What else could potentially be done to minimise the risk?	Ensure that the result of data analytics is anonymous.	

Table 7: DPIA table data analytics

@KrakenH2020

Kraken H2020

www.krakenh2020.eu

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