KRAKEN: A Secure, Trusted, Regulatory-Compliant, and Privacy-Preserving Data Sharing Platform

Silvia Gabrielli, Stephan Krenn, Donato Pellegrino, Juan Carlos Pérez Baún, Pilar Pérez Berganza, Sebastian Ramacher, and Wim Vandevelde

Abstract The KRAKEN project aims to enable the sharing, brokerage, and trading of personal data including sensitive data (e.g., educational and health records and wellbeing data from wearable devices) by returning its control to both data subjects/data providers throughout the entire data lifecycle. The project is providing a data marketplace which will allow the sharing of personal data and its usage for research and business purposes, by using privacy-preserving cryptographic tools. KRAKEN is developing an advanced platform to share certified information between users and organizations by leveraging on distributed ledger technology, promoting the vision of self-sovereign identity solutions (ensuring users' consent and data control in a privacy-friendly way), preserving security, privacy, and the protection of personal data in compliance with EU regulations (e.g., GDPR). The feasibility of the KRAKEN solution will be tested through two high-impact pilots in the education and healthcare fields.

S. Gabrielli
Fondazione Bruno Kessler, Trento, Italy
e-mail: sgabrielli@fbk.eu

S. Krenn · S. Ramacher
AIT Austrian Institute of Technology, Vienna, Austria
e-mail: stephan.krenn@ait.ac.at; sebastian.ramacher@ait.ac.at

D. Pellegrino
TX - Technology Exploration Oy, Helsinki, Finland
e-mail: donato@tx.company

J. C. Pérez Baún (✉) · P. Pérez Berganza
ATOS Spain S.A., Madrid, Spain
e-mail: juan.perezb@atos.net; pilar.perez@atos.net

W. Vandevelde
katholieke Universiteit Leuven, Leuven, Belgium
e-mail: wim.vandevelde@kuleuven.be

E. Curry et al. (eds.), *Data Spaces*, https://doi.org/10.1007/978-3-030-98636-0_6

Keywords Privacy-preserving data · Privacy-aware analytic methods · Trusted and secure sharing platforms · Self-sovereign identity · User-centric design · GDPR compliance

1 KRAKEN Overview

The KRAKEN(brokerage and market platform for personal data) project[1] is an innovation action funded by the EU H2020 program (under grant agreement no. 871473) with the main objective to develop a trusted and secure personal data platform with the state-of-the-art privacy-aware analytics methods, guaranteeing metadata privacy and query privacy and returning the control of personal data back to users.

The KRAKEN chapter mainly relates to the technical priorities of data protection, data analytics, and data management of the European Big Data Value Strategic Research and Innovation Agenda [1]. It addresses the horizontal concerns on privacy, data analytics, and data management of the BDV Technical Reference Model. It addresses the vertical concerns on cybersecurity, marketplaces for personal data platforms, and data sharing.

The main challenge to achieve this goal is to empower the citizens on the control of their own personal data, including sensitive data, and motivate the user to share this kind of data.

With this objective KRAKEN is investigating data processing mechanisms working in the encrypted domain with the aim to increase security, privacy, functionality, and scalability for boosting trust.

The first challenges KRAKEN is facing are the loss of control over data and the use of centralized identity management systems. In this sense KRAKEN is returning the control of personal data back into the hands of data subjects and data providers and its subsequent use, which includes the user consent management. Additionally, in contrast to identity management systems which follow centralized approaches involving dependencies, KRAKEN is advocating for a decentralized self-sovereign identity (SSI) management and user-centric access control to data, where the data provider has the control over their data.

Other important challenges this project is addressing are related to individual privacy and security requirements. KRAKEN will develop easy-to-understand privacy metrics and usable interfaces for end users and data subjects, and also privacy-preserving analysis based on advanced cryptography.

A basic aspect to cover when personal and sensitive data are managed and shared is the fulfillment of regulatory framework. KRAKEN addresses this regulatory challenge through General Data Protection Regulation (GDPR) [2] and eIDAS compliance, following standards for compatibility and interoperability and promoting best practices.

Furthermore, in order to motivate the user to share their data, the development of fair-trading protocols and incentive models is envisaged. KRAKEN is handling this

[1] https://www.krakenh2020.eu/

business challenge by establishing economic value and innovative business models for "personal Data Spaces" supporting the Digital Single Markets' data economy and engaging SMEs. In this way users can receive some incentive pushing them to share their data.

With the aim to generalize the KRAKEN experience to other economic sectors, KRAKEN will be demonstrated in two high-impact pilots on health and educational domains, in realistic conditions, with legal compliance, considering usability and transparency. In this sense, KRAKEN contributes to the European strategy for data, namely, the boost of the common European Data Spaces by leveraging the SSI paradigm and the cryptographic techniques. These technologies facilitate the fair management of the user data, making them available to be used by several economic domains.[2]

Additionally, the KRAKEN chapter relates to knowledge and learning enablers of the AI, Data and Robotics Strategic Research, Innovation, and Deployment Agenda [3], which can impact the future activities in AI and data.

In summary, KRAKEN is addressing all these challenges providing a sharing data marketplace that is relying on SSI services and cryptographic tools for covering the security, privacy, and user control on data. At the end KRAKEN will provide a highly trusted, secure, scalable, and efficient personal data sharing and analysis platform adopting cutting-edge technologies and leveraging outcomes from the CREDENTIAL[3] and MyHealthMyData[4] projects.

At this moment the high-level KRAKEN architecture (Fig. 1) is provided considering the three main pillars:

- The SSI paradigm providing a decentralized user-centric approach on personal data sharing. The SSI pillar comprises the SSI mobile app for storing verifiable credentials (VCs) and key material, the legal identity manager for issuing an identity of VC leveraging the eIDAS eID network and signing this VC, and the KRAKEN Web Company Tool (KWCT) web tool for VC management.
- A set of different analytics techniques based on advanced cryptographic tools that will permit privacy-preserving data analysis. The cryptographic pillar provides functional encryption (FE) and secure multi-party computation (SMPC) for protecting the sharing of data on the marketplace, a backup service for a secure key material cloud storage, and zero-knowledge proof (ZKP) protocols and proxy re-encryption (PRE) mechanisms for privacy and secure data exchange.
- A data marketplace which will allow the sharing of personal data preserving privacy when Artificial Intelligence/machine learning analysis is made. The marketplace pillar is basically built by a decentralized and distributed processor and a blockchain network for business logic management by using smart contracts.

The health and education domains were selected to demonstrate how SSI and cryptographic technologies can improve the security and privacy of personal data,

[2] https://digital-strategy.ec.europa.eu/en/policies/strategy-data

[3] https://credential.eu/

[4] http://www.myhealthmydata.eu/consortium/

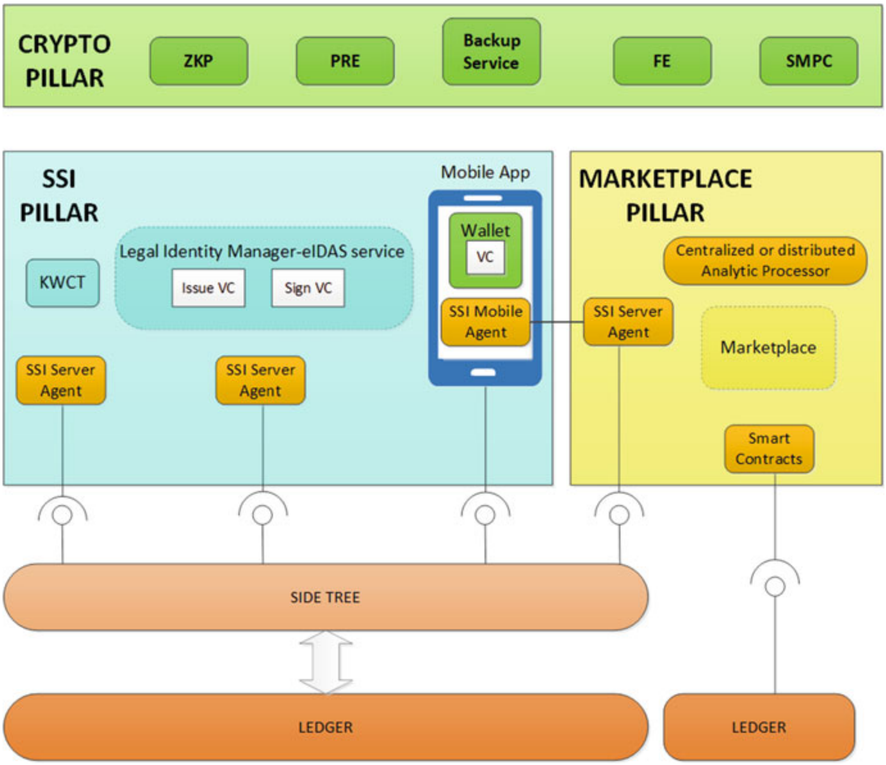


Fig. 1 High-level KRAKEN architecture

including sensitive data, when shared in a marketplace. The health scenario involves sensitive data such as biomedical and wellbeing data, which implies the use of powerful privacy-preserving techniques assuring the data are protected at all times. The education scenario involves personal data such as grades, courses, or diplomas, which can be provided to a third party in a privacy-preserving way. In both cases the use of SSI and cryptographic technologies eases the shared use of these data, assuring the data are protected and the owner has the control over the use of the data.

2 Architectures for Data Platform

2.1 KRAKEN Data Platform Architecture Overview

The design of the KRAKEN architecture is based on decentralization, cryptography, and self-sovereign identity (SSI) [4].

The architecture reflects of the user requirements related to the different data products that can be published on the platform. In the KRAKEN marketplace the users are divided into two categories: data providers and data consumers. The data providers are the users whose interest is to publish data products on the platform and earn money by granting access to data consumers. The data consumers are the users whose interest is to buy access to data products.

The data products are divided into three categories: batch data, real-time data, and analytics. Based on the type of data product, the requirements of the users change. One of the requirements that is common between all the three kinds of data products is the eligibility of the data consumer. Data providers are willing to provide their personal data only to data consumers that passed through an eligibility check. In KRAKEN this is accomplished by exploiting blockchain [5] and SSI technology.

The blockchain is the decision-making component of the platform. Through decentralization, the KRAKEN marketplace is able to provide an incorruptible mean whose duty consists in granting access to data products to eligible consumers and keep track of all the transactions in a distributed immutable ledger.

The ledger is also used to store also the policies set by the data providers to instruct the blockchain on how to filter data consumer requests. These policies are checked also against SSI verifiable credentials. To perform this check, the architecture includes an SSI agent. The SSI agent is used to check the validity of the credentials of the users that contain the needed information to be checked against the policies.

One of the requirements of the users is to be in total control of their own personal data. For this reason, the KRAKEN marketplace does not store any data product-related resources (such as the dataset files). However, data consumers need to be able to access the data. To do so, KRAKEN relies on cloud storage systems. Every data provider can choose any cloud storage system available nowadays to store their data. Once they provide the location of the data to the KRAKEN marketplace, such location is shared only with data consumers to let them download the data.

The privacy-preserving analytics data product specifically enables users to share analytics on their personal data without revealing the original data to data consumers and to any third party performing the analytics computation. The element of the architecture that makes this possible is the secure multi-party computation (SMPC) [6] network. SMPC is a technology that allows the establishment of a decentralized network capable of communicating with users exploiting a secret-sharing mechanism. This mechanism consists in encrypting the message in a way that prevents the network from obtaining the original message, but allows the network to perform computation on it and generate an encrypted result that can be decrypted only by the data consumer, still through the same secret-sharing mechanism.

The real-time data product consists of a stream of real-time messages from data providers to data consumers. This needs to happen in a decentralized manner that does not put trust in any middleman. To do so, the KRAKEN marketplace is interfaced with Streamr [7]: a peer-to-peer network for real-time data sharing that aims to become decentralized. In this specific data product, KRAKEN acts as a permission layer to filter the eligible buyers of the data product.

To interact with KRAKEN marketplace users can access the KRAKEN marketplace website. The backend server is used to store the metadata about data products that are fetched by the frontend to allow users to browse through them. The frontend is the tool used by users to perform operations on KRAKEN such as publication and purchase. Exploiting the frontend, users are able to set up policies, present VCs using an SSI wallet, and perform cryptographic processing of their datasets locally.

Payments on KRAKEN are performed using Streamr's DATA coin. DATA coin is a token available on the Ethereum[5] blockchain and on the xDai[6] blockchain. The blockchain used by the KRAKEN marketplace to run the payment smart contract is the xDai blockchain.

Data access in the KRAKEN marketplace is time based by default. The subscription to any of the data products has a parameter that specifies for how much time the data consumer can access the data product. After this time limit, access is automatically revoked by the marketplace.

An overview of the entire architecture involving data flow and analytics is shown in Fig. 2.

2.2 Enabling Decentralized Privacy-Preserving Decision-Making Using Permissioned Blockchain Technology and SSI

In the KRAKEN marketplace the selection of eligible buyers for data products is performed on a blockchain. The specific technology adopted is Hyperledger Fabric [8]. Hyperledger is an open-source community producing blockchain related software. One of them is Fabric: a technology to develop permissioned blockchain solutions. The features provided by Fabric are diverse; the ones that are specifically exploited by the KRAKEN marketplace are the permissioned consensus, the smart contracts, and the distributed immutable ledger.

Fabric is not a public blockchain; this means that nobody outside of the Fabric network is able to access the information inside the distributed ledger. The members of the network are well known and, because of the permissioned nature of the blockchain, are granted permission to participate in the network only by the already existing peers.

The feature of Fabric that enables the decision-making in the KRAKEN marketplace are the smart contracts. Data providers need to be able to declare a set of policies that need to be checked against the SSI verifiable credentials of the buyers. To enable this process, the decision-making in the KRAKEN marketplace

[5] https://ethereum.org/en/

[6] https://www.xdaichain.com/

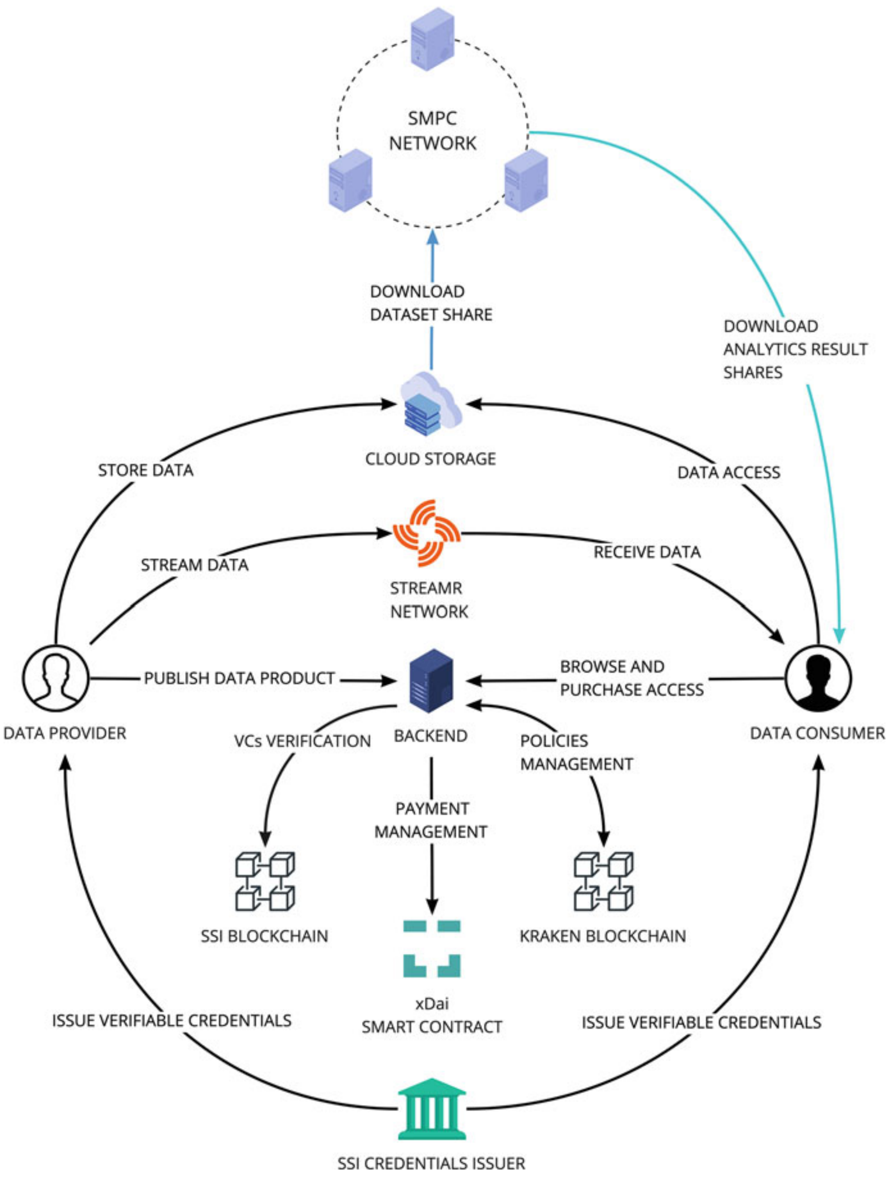


Fig. 2 Data flow and analytics on the KRAKEN marketplace architecture

is programmed using smart contracts. Because of the decentralized nature of the system, this decision-making does not depend on a single party but on a set of organizations that constitute the KRAKEN consortium. In this way the corruptibility of the system is substantially decreased if we compare it to centralized solutions.

The need of the system to have a decentralized decision-making must be joined with the possibility of storing the transactions in a way that nobody, in a later moment, is able to modify or delete it. The ledger is the storage place for information. All the transactions happening on the blockchain are stored on the ledger, including the data product publication and the purchases of eligible buyers. The ledger is not only private but also distributed and immutable. Because of its immutability, it represents the best fit for the purposes of anti-tampering and auditability.

The decentralized decision-making process needs another element to be secure. The information provided to the system has to be verifiable and this needs to happen in a way that preserves the privacy of the users. This need in the KRAKEN marketplace is fulfilled by the SSI technology. Through SSI, users are able to provide verifiable information to the system in the form of a VC.

VCs, in the scope of self-sovereign identity, are certificates released by institutions and organizations to state a specific characteristic of a person, for example, nationality, affiliation to a company or organization, or the fact that one is not underage. This kind of credential is made with the scope of revealing only a specific characteristic of an individual and nothing more, for example, the affiliation to a company does not necessarily also reveal the role that a person has in the company. The credentials are checked using the SSI blockchain. In this way, the privacy of buyers is also protected against its own organization that cannot know when and how the credential is used and cannot block it if not by revocation.

3 Real-Time Data Sharing Using Streamr: A Decentralized Peer-to-Peer Network

One of the data products of the KRAKEN marketplace is the real-time data product. This product consists of streams of real-time messages published by the data provider and received by the data consumers. The streams are enabled by the Streamr network: an open-source peer-to-peer network.

Streamr is a project that aims to realize a decentralized worldwide network for real-time data sharing. In its current state, Streamr is not fully decentralized yet, but it is already a peer-to-peer publish-subscribe network for real-time data transfer. It works with IoT devices, applications, and anything with an Internet connection that can run the Streamr client software.

The network is formed by a set of broker nodes. These nodes are intended to be installed on always-on computers connected to other nodes to route the traffic. The governance of the network is performed by a smart contract on the Ethereum blockchain. All the information regarding coordination, permissioning, and access control of data streams is saved on this smart contract. The actual transfer of data happens off-chain on the Streamr network that benefits from the “network effect” as with the increasing number of nodes, the scalability increases as well.

Through Streamr, users can publish streams of data and not worry about establishing an infrastructure to reach the subscribers. The subscribers can subscribe to the streams in a decentralized way by paying with cryptocurrencies like DATA coin. All of this happens on the Streamr marketplace, but while Streamr successfully performs a selection of buyers based on the payment, it cannot select them based on the eligibility criteria set by the data providers. Here is where KRAKEN gets into action. In addition to providing the other two kinds of data product, in the case of stream data, the KRAKEN marketplace acts as a filter in the already existing pub-subsystem implemented in Streamr where the selection of buyer does not depend solely on the payment but also on the matching of the policies set by the data providers with the VC provided by the data consumer.

4 Privacy, Trust, and Data Protection

In the following we will provide a high-level overview of the cryptographic measures taken by the KRAKEN architecture to guarantee the privacy of the user's data while simultaneously offering high authenticity guarantees to the data consumer. The interplay of all cryptographic primitives discussed in the following is also illustrated in Fig. 3.

Multi-party Computation Secure multi-party computation (SMPC), introduced by Yao [6], has become an interesting building block for many privacy-preserving applications. SMPC allows a group of nodes to jointly perform a computation on secret inputs, without revealing their respective inputs to the remaining nodes in the network or any other third party. More precisely, SMPC guarantees that for a node following the protocol specification, even potentially malicious other parties cannot infer anything about the node's input, except for what can already be inferred from the output of the computation and the malicious parties' inputs. Furthermore,

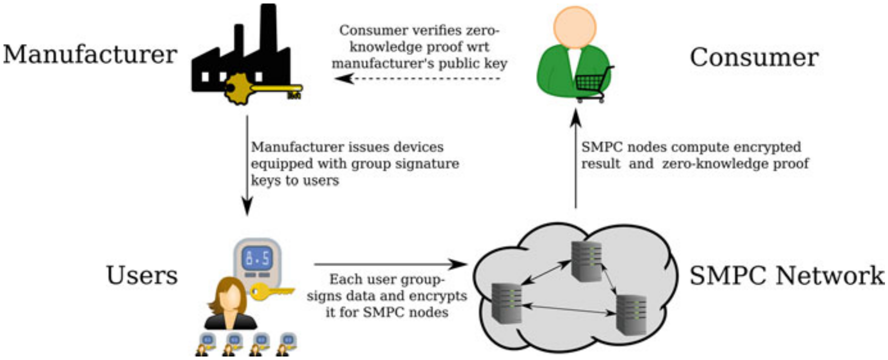

Manufacturer
Consumer verifies zero-knowledge proof wrt manufacturer's public key
Consumer
Manufacturer issues devices equipped with group signature keys to users
SMPC nodes compute encrypted result and zero-knowledge proof
Users
8.5
Each user group-signs data and encrypts it for SMPC nodes
SMPC Network

Fig. 3 Overview of the KRAKEN cryptographic architecture

the correctness of the computation can be guaranteed as long as a sufficiently large fraction of the nodes behave honestly.

However, while giving high privacy guarantees to the data provider, classical approaches to secure multi-party computation do not directly fulfill all relevant requirements in the context of KRAKEN. On the one hand, SMPC cannot give authenticity guarantees for the inputs provided by data providers. On the other hand, classical approaches to secure multi-party computation do not directly enable the data provider to verify the correctness of the computation. In the following we will briefly discuss KRAKEN's approaches to solve these two interdependent issues.

End-to-End Authenticity For many application scenarios, the value of data and analytics performed by the KRAKEN platform are highly dependent on the authenticity of the results delivered to a buyer. A natural way to achieve authenticity would be to let the users sign their input data before handing it over to the SMPC nodes. For sensitive data, this signature could be issued directly by a sensor or device owned by the user, which would then guarantee that only data certified by trusted devices (e.g., from a certain manufacturer) would be processed by the SMPC nodes. However, this straightforward approach might violate the users' privacy: verifying the authenticity of input data using the corresponding public key reveals data belonging to the same user and might also allow to identify a user. To avoid this re-identification problem, KRAKEN deploys so-called group signatures [9]: such signatures allow a user to sign messages on behalf of a group while remaining anonymous. That is, the verifier will only be able to check that the message has been signed by some member of group, but not to identify the specific signer. Group membership is controlled by a group manager, with whom any user wishing to join the group needs to execute a registration process. In our context, device manufacturers could now provide each device with a group signature key, which is used to sign, e.g., sensor data. The SMPC nodes as well as the data consumer can now verify the correctness of the signatures using the group manager's public key to verify the authenticity of the input data, without compromising the user's privacy.

On a technical level, it is worth noting that group signatures come with a so-called opening functionality, which allows a predefined third party to identify the signer in case of abuse. To avoid any privacy bottleneck, all key material will be sampled in a way that disables this functionality under standard complexity theoretical assumptions, resulting in a scheme akin to Intel's enhanced privacy ID (EPID) signatures [10].

Correctness With SMPC and group signatures, KRAKEN can give high authenticity guarantees to the data consumer, as long as sufficiently many SMPC nodes are trusted. However, the approach discussed so far neither allows one to drop this assumption, nor does the data consumer have cryptographic evidence about the correctness of the data, meaning that the results could not credibly be presented to any third party. Again, a naive solution could be to let the SMPC nodes sign their respective outputs together with the evaluated function, enabling the data consumer to forward results to third parties, as long as sufficiently many SMPC nodes are assumed to be honest. The approach taken in KRAKEN is different, such that any trust assumptions on the SMPC network can be dropped with regard to the authenticity of the results. Namely, KRAKEN will attach so-called non-interactive zero-knowledge proofs of knowledge [11, 12] certifying the correctness of the provided outputs. Such cryptographic proofs allow one to prove the correctness of a claim without revealing any information than what is already revealed by the claim itself. For KRAKEN, the zero-knowledge proofs will thus cryptographically prove that, starting from private input values which have been signed using a group signature scheme, the function provided by the data consumer has been correctly computed.

Trust Assumption Overall, KRAKEN minimizes the trust assumptions to the best extent possible. Regarding privacy, no user data is revealed to any single entity in the architecture, and also the number of collaborating SMPC nodes necessary to break privacy can be adjusted. Any other ways to break privacy would require compromising communication channels or group signature schemes, for which formal security proofs exist. On the other hand, regarding authenticity, the necessary trust of the data buyer is minimized by the use of group signature schemes and zero-knowledge proofs, and all guarantees can be based solely on the security of the initial signatures on the user's data. For a more detailed discussion about the cryptographic architecture underlying KRAKEN and a detailed privacy analysis following the LINDDUN framework, we refer to Koch et al. [13].

5 Sharing by Design, Ownership, and Usage Control

The most widely deployed approach for data sharing in the cloud, e.g., Google Drive, allows users to upload and share data with others, but beyond the trust put into the cloud provider, no security guarantees can be achieved. While secure communication channels are used between users and the cloud provider, these systems are unable to ensure end-to-end security between users. In an ideal scenario, however, the data owner has complete control over the data and cryptographic schemes to ensure confidentiality of the data with respect to anyone except authorized users. Importantly, this also means that the data is protected against adversarial access by the cloud provider and others. Such strong security guarantees are nontrivial to implement in a cloud-based document and data sharing setting. Approaches based on the use of public-key encryption quickly turn into non-scalable solutions due to the complexity of the involved key management. The use of more advanced techniques such as proxy re-encryption [14] or identity-based encryption [15] often runs into issues when deployed in practice. With these techniques key management remains a crucial part of the system and requires users to constantly interact to exchange key material.

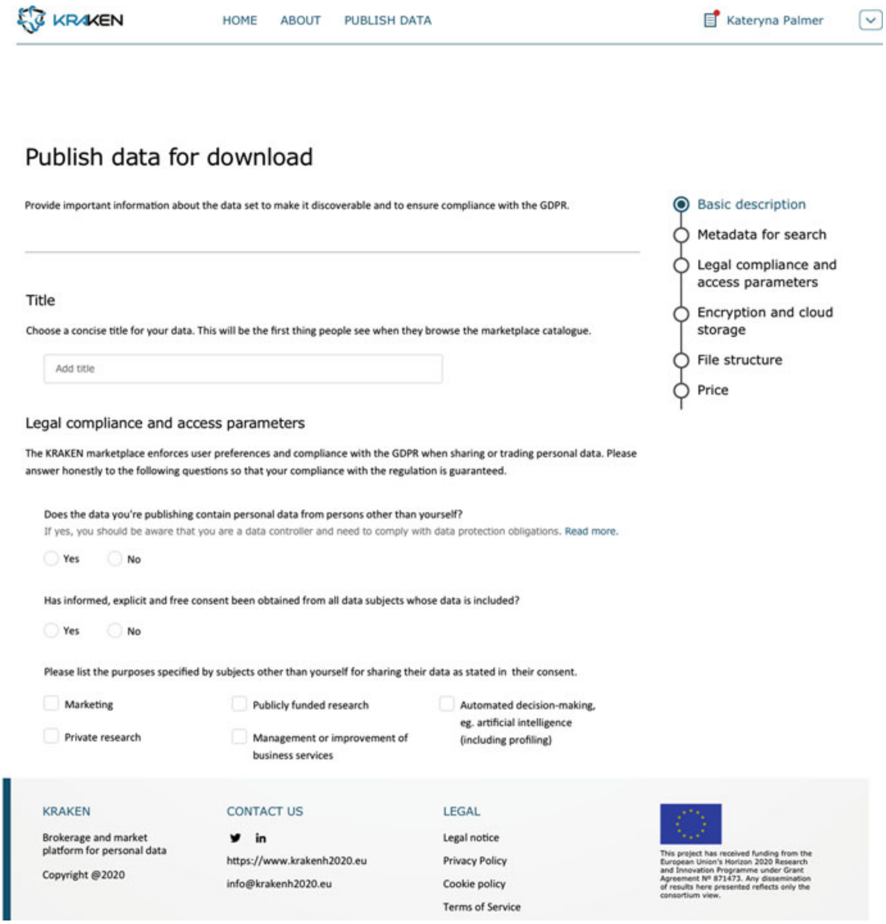
KRAKEN follows a different approach for data sharing that leverages SMPC techniques and the SMPC nodes that are deployed as part of the effort to enable privacy-preserving computation on data. To some extent, data sharing can be seen as a special case of computation on encrypted data. By leveraging the SMPC network, the key management issues can be solved by handling these tasks via the SMPC network [16]. Thereby, the SMPC networks give rise to a scalable system for user-controlled data sharing with end-to-end security. Users are only required to trust one of the SMPC nodes to execute the protocols honestly while keeping their data safe from cloud providers and potential attackers.

The most interesting aspect of running the key management inside the SMPC network is the user's ability to define access policies that after initial verification by the blockchain network are verified and enforced by the SMPC nodes. Similar to a domain-specific language for trust policies [17], users will be able to express their access policies within a policy language designed within KRAKEN [18]. Before sharing data with the receiver, the MPC nodes evaluate if the data receiver satisfies this policy and only then produce the corresponding keys for accessing the data. In comparison to approaches based on encryption schemes with fine-grained access control, users are not required to be online for processing keys within the SMPC network. Additionally, the SMPC network can be extended to provide accountability proofs that give data owners a way to check that the SMPC network validated the access policy [19].

For sensitive data, users are empowered to run their own SMPC node. Especially when dealing with eHealth data, hospitals may host one SMPC node on their own infrastructure. In this case, users do not need to put any trust into any of the other SMPC nodes. Thereby, all trust issues are alleviated. For users unable to host SMPC nodes themselves, privacy-focused organizations may help to distribute trust assumptions and requirements, thereby reducing the risk of data compromise.

5.1 User-Centric Data Sharing

The widespread adoption of the KRAKEN platform depends on new types of user behavior. Users need to understand the value of their personal data [20], the extent to which they are able to control their use, and how they are able to do that. The vision leading the KRAKEN design is to empower users in their ability to control their own data and to promote knowledge about the management of personal data and the distribution of value generated from data. The issue of user adoption has to do with the quality of user experience with the working platform provided; that is why in KRAKEN designers apply user-centric design approaches to understand and assess the needs and preferences of potential data consumers and data providers, in order to realize working prototypes fitting those needs. However, in KRAKEN we are also aware that in order to fully realize the innovation potential of our solution, we need to attract broad masses of users to join and engage with our platform. This requires more than a just a usable working solution, since the key mechanisms explaining how the blockchain and a privacy-preserving data sharing platform work may not be self-explanatory to a standard user. The aim is therefore that of favoring a gradual adoption of our platform, by supporting and gaining user's



Publish data for download

Provide important information about the data set to make it discoverable and to ensure compliance with the GDPR.

● Basic description
○ Metadata for search
○ Legal compliance and access parameters
○ Encryption and cloud storage
○ File structure
○ Price

Title

Choose a concise title for your data. This will be the first thing people see when they browse the marketplace catalogue.

Add title

Legal compliance and access parameters

The KRAKEN marketplace enforces user preferences and compliance with the GDPR when sharing or trading personal data. Please answer honestly to the following questions so that your compliance with the regulation is guaranteed.

Does the data you're publishing contain personal data from persons other than yourself?
If yes, you should be aware that you are a data controller and need to comply with data protection obligations. Read more.

○ Yes ○ No

Has informed, explicit and free consent been obtained from all data subjects whose data is included?

○ Yes ○ No

Please list the purposes specified by subjects other than yourself for sharing their data as stated in their consent.

□ Marketing
□ Private research
□ Publicly funded research
□ Management or improvement of business services
□ Automated decision-making, eg. artificial intelligence (including profiling)

KRAKEN
Brokerage and market platform for personal data
Copyright @2020

CONTACT US
https://www.krakenh2020.eu
info@krakenh2020.eu

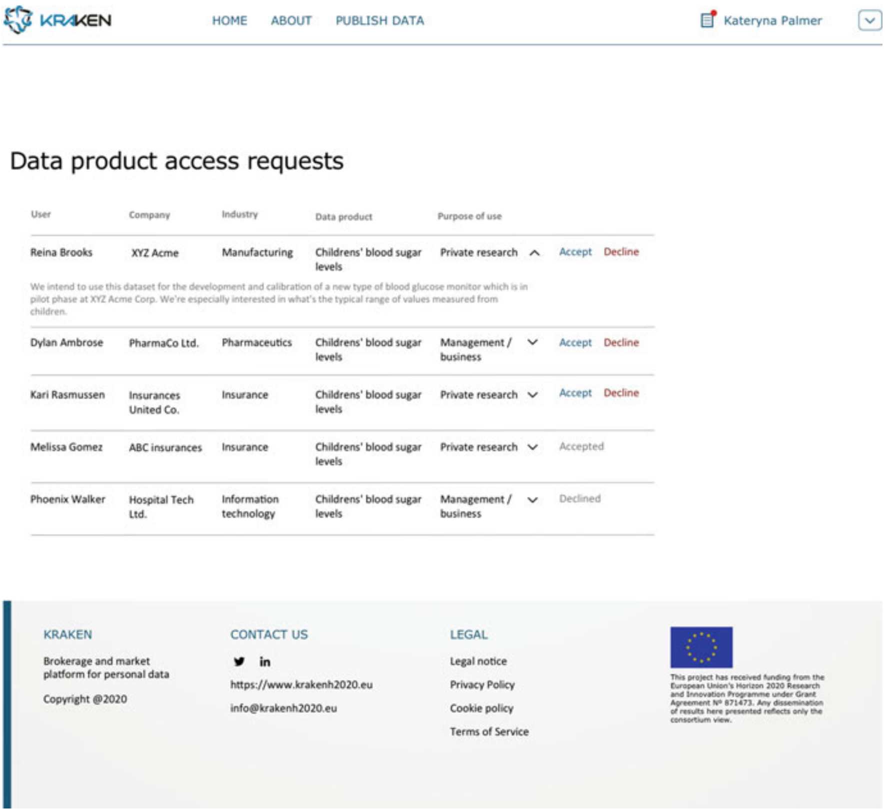
LEGAL
Legal notice
Privacy Policy
Cookie policy
Terms of Service

This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement Nº 871473. Any dissemination of results here presented reflects only the consortium view.

Fig. 4 Mockup of screen enabling a data provider to specify legal compliance and access parameters while creating a data product

trust through the provision of specific built-in privacy-preserving features able to foster increased utilization and sustained data sharing behavior over the long term [21]. The KRAKEN platform will incorporate easy-to-use and easy-to-learn privacy metrics as well as interfaces enabling data sharing through the platform in the most effective and efficient way, ensuring at the same time privacy and safety in its use. Providing to data providers the possibility of fully controlling access to their data by third parties, for example, by specifying legal compliance and access parameters to a data product (Fig. 4) as well as by being able to accept or decline access requests to a data product (Fig. 5), will help to eliminate users' concerns about privacy controls [22].

The KRAKEN platform and marketplace will enforce these consumer-centered features and contribute to educate users on how to best keep control of access



Data product access requests

User	Company	Industry	Data product	Purpose of use		
Reina Brooks	XYZ Acme	Manufacturing	Childrens' blood sugar levels	Private research	^	Accept Decline
We intend to use this dataset for the development and calibration of a new type of blood glucose monitor which is in pilot phase at XYZ Acme Corp. We're especially interested in what's the typical range of values measured from children.						
Dylan Ambrose	PharmaCo Ltd.	Pharmaceutics	Childrens' blood sugar levels	Management / business	˅	Accept Decline
Kari Rasmussen	Insurances United Co.	Insurance	Childrens' blood sugar levels	Private research	˅	Accept Decline
Melissa Gomez	ABC insurances	Insurance	Childrens' blood sugar levels	Private research	˅	Accepted
Phoenix Walker	Hospital Tech Ltd.	Information technology	Childrens' blood sugar levels	Management / business	˅	Declined

KRAKEN

Brokerage and market platform for personal data

Copyright @2020

CONTACT US

https://www.krakenh2020.eu

info@krakenh2020.eu

LEGAL

Legal notice

Privacy Policy

Cookie policy

Terms of Service

This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement Nº 871473. Any dissemination of results here presented reflects only the consortium view.

Fig. 5 Mockup of screen where a data provider can visualize, accept, or decline data product access requests received by the KRAKEN marketplace

to their data. It is likely that consumers' willingness to share their data is also affected by factors such as the end purpose of the third party (i.e., making money or research purposes); therefore, enabling mechanisms to support decision-making by the data providers will sound more appealing to a wider audience of potential users of the platform. More reflection is also needed on how to further incentivize data sharing through our platform, by taking into account that some categories of data providers, in the biomedical or healthcare domain for instance, might place greater value on receiving non-monetary forms of compensation (e.g., free treatment, shared research results) instead of value tokens or cryptocurrencies. These examples of design options stress the importance of understanding and monitoring the needs and preferences of KRAKEN users to enable a more successful coevolution and adoption of the data sharing platform, by optimizing and better deploying the advanced technical capabilities of our solution with their users' behaviors.

6 Compliance with Data Protection Framework

This section will give a short overview on the approach of KRAKEN regarding compliance with the relevant data protection framework (i.e., the GDPR). The focus therefore lies on the application of the GDPR [2], even though there are several other frameworks that apply to the KRAKEN platform and accompanying technologies (e.g., the eIDAS Regulation, eCommerce Directive, and future Data Governance Act). In order to ensure that the data subject is adequately protected, and their data are processed fairly and securely, KRAKEN goes beyond a minimum application of the relevant rules by applying a proactive approach toward compliance. This is achieved by considering and integrating important data protection principles and concepts from the outset rather than as an afterthought. Such an approach enhances trust in, and acceptance of, the KRAKEN platform, allowing citizens to benefit from the sharing of their own personal data.

6.1 Data Protection Principles and Their Implementation

The data processing activities in the context of the KRAKEN platform can be divided into two main categories: data processing activities by the KRAKEN platform for the purpose of providing the KRAKEN platform service (i.e., the processing of account data[7]) and data processing activities by the data consumer for their own specific purposes (i.e., processing of content data[8]). This is an important distinction for the application of the GDPR because, as a result, the KRAKEN platform acts as a controller for the processing of account data, while the data consumer acts as a controller for the processing of content data. The implementation of the data protection principles of article 5 GDPR ("principles relating to processing of personal data") will therefore differ depending on the context of the data processing activities. The following overview will mainly focus on the processing of content data by the data consumer since the application of the data protection principles to the processing of account data by the KRAKEN platform is more straightforward in nature.

6.1.1 Lawfulness, Fairness, and Transparency

Lawfulness The principle of lawfulness imposes that all processing activities must comply with the law and must rely on a legitimate legal basis found in article 6

[7] Account data refers to data relating to the user profile necessary to provide the KRAKEN platform service (e.g., name, e-mail address, country of residence, etc.).

[8] Content data refers to data that is published on the KRAKEN platform for sharing with data consumers (e.g., educational data or health data).

GDPR ("lawfulness of processing"). In the context of KRAKEN, the processing of content data by the data consumer always relies on the valid consent of the data subject. Consequently, in order to share personal data on the KRAKEN platform, it is necessary to have first obtained valid consent from the data subject.

According to the GDPR, consent is only considered valid if it is (a) *freely given*, *(b) specific*, *(c) informed*, and (d) *unambiguous:*

- *Freely given:* the data subject must have a genuine and free choice; there should be no imbalance of power between the parties involved and the data subject must be able to exercise their free will.
- *Specific:* consent should be given in relation to one or more specific purposes, providing the data subject with a degree of control and transparency. There should be granularity in the consent request and relevant information should be layered in a way that separates it from other information. The data subject should always be able to understand for which specific purpose consent is given.
- *Informed*: the data subject must be properly informed in an intelligible way, using clear and plain language before giving their consent. This should include information about the controller, processing activities, specific purposes, data subject rights, and more.
- *Unambiguous*: consent must constitute a clear affirmative action and must show an unambiguous indication of the data subject's wishes; silence, pre-ticked boxes, and inactivity do not constitute valid consent [23].

In the context of the KRAKEN platform, valid consent is obtained through the user interface and dynamic consent management tool. In the scenario where an institution publishes personal data of data subjects on the KRAKEN platform (e.g., a hospital), they must first confirm that valid consent has been obtained from the data subjects related to the dataset. If an institution wishes to share personal data for different purposes than was included in the original consent, they must obtain new valid consent from the data subjects before proceeding with the publication of the dataset.

In the scenario where a data subject publishes their own personal data on the KRAKEN platform, they are guided through the user interface that allows them to give consent in a *free*, *specific*, *informed*, and *unambiguous* manner.

Firstly, the data subject has a real choice and control over whether or not to publish their personal data using the KRAKEN platform. Consent is in no way a non-negotiable condition that is tied to other agreements and the data subject can freely exercise their own will.

Secondly, the data subject is able to select the types of actors that can access and process the data (e.g., public research centers, private companies, governments, etc.) and the specific purposes of processing (e.g., marketing, private research, public research, etc.) in a granular way. Different from a more traditional processing context, it is the data subject that determines the permissions for data processing (incl. specific purposes) when publishing personal data (Fig. 5). Data consumers must also specify and confirm their own intended processing purposes, which are then compared with the specified permissions of the data subject to see whether there is a match. This gives the data subject the necessary control and transparency as to the specific purposes of processing. In order to further safeguard the purpose limitation principle, blockchain technology is used to only allow access to data products by eligible data consumers. In case a data consumer is considered to be ineligible based on a mismatch between the specified permissions, they can still request access to the data product which the data provider can then accept or decline (Fig. 5).

Thirdly, the data subject will be properly informed about the types of processing actors, purposes of processing activities, the possibility to withdraw consent at any time without detriment, and their data subject rights. This information is provided by, in addition to a clear privacy policy, the inclusion of disclaimers and references to additional information throughout the data publication process. In line with the transparency principle, the interface and related information are presented in a concise, transparent, intelligible, and easily accessible form, using clear and plain language. Furthermore, the dynamic consent management tool allows the data subject to manage and modify their consent preferences at any time. Consent can therefore be changed or withdrawn according to the will of the data subject.

Lastly, providing consent on the KRAKEN platform requires multiple affirmative actions by ticking boxes and progressing through the data publication process.

Fairness This principle determines that personal data must not be processed in a way which unreasonably infringes upon the fundamental right to the protection of personal data of the data subject. Processing can therefore be lawful, but still considered unfair with respect to the means foreseen and the reasonable expectations of the data subject. It is essential that the envisioned processing activities, specific purposes, and data subject rights are always clear to the data subject [24].

Transparency As a core data protection principle, transparency applies to all stages of the processing lifecycle. The GDPR makes clear that all information and communications on the processing of personal data should be provided to the data subject in a concise, transparent, intelligible, and easily accessible form while using clear and plain language. The aim is to ensure that data subjects are exhaustively aware of the processing activities and extent of processing relating to their personal data. Thus, the principle of transparency is closely linked to concepts such as valid consent, fairness, information obligations, and the data subjects' rights provided by the GDPR.

The principles of fairness and transparency are also largely implemented by the measures mentioned above, with a special focus on ensuring that the envisioned data processing activities and purposes are in line with the reasonable expectation of the data subject. Additionally, the KRAKEN platform will include easy-to-use privacy metrics that enable the data subject to be aware of their privacy risks at all times.

6.1.2 Purpose Limitation, Data Minimization, and Storage Limitation

Purpose Limitation This principle states that personal data may only be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Purposes should therefore be sufficiently specific and not merely based on broad or vague concepts or notions. They must also be made explicit to the data subject in a clear and intelligible way before any processing activity takes place (cfr. the principle of transparency).

As noted before, it is the data subject that determines the permissions for data processing (incl. specific purposes) when publishing personal data on the KRAKEN platform. It is then up to the data consumers to specify and confirm their own intended processing purposes, which must match with the purposes specified by the data subject. The data consumer, acting as a controller under the GDPR, has to comply with their obligations under the GDPR, including the principle of purpose limitation. Consequently, they may only process the acquired data in accordance with the purposes specified by the data subject.

Data Minimization The data minimization principle means that personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed. In essence, this principle asks whether the same purpose can be achieved with a more limited collection of personal data. It is therefore intrinsically linked to the purpose limitation principle, as it is an application of the principle of proportionality in relation to the specified purposes.

With regard to the processing of content data, this principle must be complied with by the data consumer that acts as a controller. This can be achieved by only requesting access to strictly necessary data and periodically reviewing whether the personal data they process are still adequate, relevant, and limited to what is necessary for the specified purposes. If the answer is negative, unnecessary personal data should be deleted and incorrect or incomplete data should be rectified. With regard to the processing of account data, the KRAKEN platform only processes what is strictly necessary to provide the KRAKEN platform service in a secure and privacy-friendly way. This encompasses the processing of personal data such as the name, e-mail address, country of residence, etc.

Storage Limitation According to this principle, which is closely linked to the principles of purpose limitation and data minimization, personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. Consequently, once personal data are no longer necessary for the specified purposes, they must be removed from storage or irreversibly de-identified.

Similar to the application of the data minimization principle, it is up to the data consumer acting as a controller to conduct periodic reviews and establish storage, retention, and deletion policies prior to data collection. The KRAKEN user interface allows for the specification of storage periods by the user, which the data consumer must comply with.

6.1.3 Accuracy, Integrity, and Confidentiality

Accuracy The principle of accuracy says that personal data should be accurate and, where necessary, kept up to date. With regard to content data, the data consumer that acts as a controller should keep data accurate at all stages of the processing lifecycle, taking every reasonable step to erase or rectify inaccurate personal data without delay. This can be achieved through review mechanisms and the exercise of the data subject's right to rectification and erasure. With regard to account data, the KRAKEN platform should aim to keep the relevant account details accurate and up to date.

Integrity and Confidentiality This principle states that personal data must be processed in a manner that ensures appropriate security of the personal data. The aim is to protect personal data against unauthorized or unlawful processing, accidental loss, destruction, or damage.

The data consumer that acts as a controller in relation to content data should take steps to implement appropriate technical and organizational measures, such as clearly defined access policies, systemic quality controls, and technical features against data breaches. The level of security should be periodically reviewed to ensure constant protection of personal data. The KRAKEN platform, on the other hand, should also aim to secure the integrity and confidentiality of account data.

Additionally, in order to secure the storage and transfer of personal data, the KRAKEN project introduces appropriate security measures. Because no data products are stored on the KRAKEN platform, but rather by external cloud service providers, strong end-to-end encryption is in place. The use of privacy-preserving analytics also safeguards the integrity and confidentiality of personal data by enabling users to share analytics on their personal data without revealing the initial data. Finally, the use of blockchain technology as a decision-making component allows KRAKEN to only allow access to data products by eligible data consumers. The same blockchain technology stores policies set by the data provider which are checked against SSI VCs of the data consumer by making use of smart contracts.

6.1.4 Accountability

The principles of accountability relate to all previous principles by stating that the controller is responsible for, and must be able to demonstrate compliance with, the other data protection principles.

This means that the controller is responsible for actively implementing appropriate technical and organizational measures in order to promote and safeguard the protection of personal data and to be able to demonstrate that the processing activities are conducted in accordance with the GDPR. In this context, the controller is obliged to keep records of processing activities under its responsibility in order to promote and demonstrate compliance. This also applies to the legal basis of consent, which the controller should also be able to demonstrate according to article 7 GDPR ("conditions for consent"). For these reasons, it is important that the data consumer that acts as a controller implements record-keeping systems for possible audits and inspections. The KRAKEN platform also contributes to the accountability of data consumers by storing evidence of consent through the dynamic consent management application and the tracking of transactions through the blockchain. KRAKEN also informs data consumers about their obligations under the GDPR and provides a system that allows data consumers to clearly stay within the boundaries of valid consent, such as the purposes specified by the data provider.

6.2 The Exercise of Data Subject Rights

Under Chapter III of the GDPR, data subject is entitled to exercise and request their rights vis-à-vis the responsible controller. In the context of KRAKEN, the exercise of data subject rights has two dimensions: vis-à-vis the KRAKEN platform in relation to account data and vis-à-vis the data consumer that acts as a controller in relation to content data. Data subjects are informed about their rights under the GDPR at several points, for example, at profile creation and publication of a data product, in addition to the privacy policy.

With regard to the exercise of data subjects' rights vis-à-vis KRAKEN, data subjects may request their rights by using the KRAKEN contact details and communication channels provided to them. The right to erasure of personal data can be exercised through a profile deletion process, which erases their personal data held by KRAKEN.

For the exercise of data subject rights vis-à-vis the data consumer that acts as a controller, KRAKEN provides data subjects with the appropriate contact details and communication tools. In this context, KRAKEN acts as a communication channel in order to exercise data subject rights, but the requests must be granted by the data consumer. In any case, the possibility to exercise specific data subject rights is subject to the conditions and exceptions of the GDPR, which must be assessed by the data consumer.

6.3 The KRAKEN Approach Toward Data Monetization

Under the EU framework, there does not yet exist legislation that explicitly regulates the monetization of personal data. However, existing legislation applicable to the processing of personal data (i.e., the GDPR) may provide some initial guidelines. From a GDPR point of view, the discussion on the monetization of personal data is quite straightforward. The GDPR does not make specific mention of the monetization of personal data, but since these activities are in fact processing activities in the form of personal data transfers between parties, in exchange for a monetary reward, the GDPR applies as if it would to any other processing activity. The lack of an explicit prohibition means that the monetization of personal data is, in principle, allowed under the GDPR, provided that all principles and provisions are complied with. The question of whether the monetization of personal data is allowed under the GDPR thus becomes a question of compliance. Additionally, when personal data has been fully de-identified through anonymization, the processing of this data will fall outside the scope of the GDPR, which means that the accompanying legal obligations do not have to be complied with.

One of the main objectives of KRAKEN is to enable data subjects to benefit from the processing of their own personal data (e.g., a monetary reward) while still leaving data subjects in control over those data. The KRAKEN platform offers the possibility for data consumers to find relevant personal data for specific processing activities in exchange for compensation. It is important to note that transactions on the KRAKEN platform do not rely on a transfer of ownership rights over personal data (i.e., a transfer of data ownership). The data subject still remains the "owner" of their personal data and they are merely compensated for providing permission to the data consumer to process their personal data for predefined purposes and within the limits of the informed consent given by the data subject. In this sense, the KRAKEN platform merely facilitates the coming together of data providers and data consumers, with the added value of compensating the data provider.

7 Business Challenges

The KRAKEN project aims to release the marketplace of reference for sharing, brokerage, and trading personal data, based on the self-sovereign principle to ensure a user-centered approach for the management of sensitive data. From a business perspective such marketplace needs to generate value for the data providers by offering them mechanisms to evolve toward self-sovereign identity on one hand and by offering added-value services to let them generate revenues on the other hand.

In a digital world the use of digital credentials is required for a huge variety of services, from those provided by public administration including education, health, mobility, and tax declaration to those provided by private organizations such as financial, entertainment, and other services which need to verify the source and integrity of those credentials.

Digital identity is experiencing growing relevance over the last years, changing the way that citizens interact with public institutions and by extension with the private sector as well. There are market drivers that have been stimulating the development and adoption of digital identity in recent years such as the increasing number of online services (related to mobility, smart cities, digital governance etc.) which entails protective supervision of digital certification systems to properly guarantee data security and muster citizenship trust.

This scenario has brought the development of the self-sovereign identity (SSI) that states the right of individuals to control their own data without the involvement of a third party. Therefore, a new paradigm with three main stakeholders emerges:

the individual who owns and manages their digital identity, the issuer who is able to certify a specific attribute of the individual, and the verifier who requests some of these attributes.

Blockchain is the technology which has allowed to take digital identity one step further. Thanks to the immutability, dis-intermediation, and transparency of blockchain, the self-sovereign identity (SSI) paradigm has become a reality allowing users the control and portability of their data securely.

Now, individuals have the control of a huge amount of data of greatest interest for public and private institutions that can be directly or indirectly monetized through personal data marketplaces. In this context a variety of stakeholders from companies and research institutions to citizens and public administration can exchange data in a secure way and obtain a reward (monetary or not monetary). This business model releases a value proposition for all stakeholders involved by enabling the decentralized exchange of data using blockchain technologies; on one hand the use of digital identity reduces the clerical work and facilitates the interoperability among different organizations, increasing the efficiency of administrative processes; on the other hand decentralization guarantees control and integrity of data by the data owners which possess their digital wallet and decide how, when, and with whom to share the data.

The KRAKEN project takes the leadership of data marketplace evolution focusing on healthcare and education sectors, although the resulting platform could be extended to a variety of markets and business cases.

Both current healthcare and education marketplace scenarios share many characteristics. There are decentralized options to manage and share data to users but without monetization mechanisms (beyond the fact of accessing the service for free or incentive mechanisms related to gamification), with the companies being able to get revenues from data commercialization. Both types of marketplaces suffer from poor interoperability among services and they need to explore new business models enhancing aspects such as pricing and rewarding strategies.

KRAKEN aims to disrupt data marketplace market by releasing a strong value proposition based on providing added-value monetization opportunities both for organizations and individuals, guaranteeing data control by data owners and a secure and GDPR compliance data access. The KRAKEN value proposition also will empower data providers and organizations as data unions by removing the intervention of third parties. With regard to healthcare market, KRAKEN will drive the market one step further in the field of personalized medicine and telemedicine development around the concept of real-world data (RWD) [25] by facilitating data transaction at affordable cost to improve and extend traditional studies in the case of researchers and to foster innovation and AI-based applications in the case of IT companies.

From a business perspective the launch and adoption of data marketplace relies upon two aspects which feed each other: on one hand they need to provide attractive value propositions to engage data providers which will benefit from the platform, and on the other hand they need to develop mechanisms to generate economic value to incentivize stakeholders. KRAKEN addresses both issues by analyzing different

B2C and B2B business models to be applied in different phases of the process able to generate monetary and non-monetary revenues. The engagement activities take place from the very beginning of the project by open KRAKEN deployment to entities including their use case for testing. Additionally, the individual users will be engaged through the "data for services" agreement facilitating the matching between data provision and the access to services and rewards (e.g., discount on insurance premium or access to innovative data-driven services) as well as contribute to aggregated data products getting reimbursement for it. KRAKEN will democratize the data market economy by establishing mechanisms to effectively redistribute monetary revenues among all parties including individuals which are indeed the main data generators.

Acknowledgments The KRAKEN project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement no. 871473.

References

1. Zillner, S., Curry, E., Metzger, A., Auer, S., & Seidl, R. (2017). *European big data value strategic research & innovation agenda*. Big Data Value Association.
2. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 19/1.
3. Zillner, S., Bisset, D., Milano, M., Curry, E., García Robles, A., Hahn, T., Irgens, M., Lafrenz, R., Liepert, B., O'Sullivan, B., & Smeulders, A., (eds) (2020). *Strategic research, innovation and deployment agenda - AI, data and robotics Partnership. Third Release. September 2020, Brussels. BDVA, euRobotics, ELLIS, EurAI and CLAIRE.*
4. Der, U., Jähnichen, S., & Sürmeli, J. (2017). Self-sovereign identity - opportunities and challenges for the digital revolution. *ArXiv*, abs/1712.01767.
5. Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. Accessed March 31, 2021, from https://bitcoin.org/bitcoin.pdf
6. Chi-Chih Yao, A. (1982). Protocols for secure computations (Extended Abstract). *FOCS* (pp. 160–164).
7. Streamr. (2017). *Unstoppable data for unstoppable apps: DATAcoin by Streamr*. Accessed March 31, 2021, from https://s3.amazonaws.com/streamr-public/streamr-datacoin-whitepaper-2017-07-25-v1_1.pdf
8. Androlaki, E. (2018). *Hyperledger fabric: A distributed operating system for permissioned blockchains*. Accessed March 31, 2021, from https://arxiv.org/pdf/1801.10228.pdf
9. Chaum, D., & van Heyst, E. (1991). Group signatures. *EUROCRYPT* (pp. 257–265).
10. Brickell, E., & Li, J. (2010). Enhanced privacy ID from bilinear pairing for hardware authentication and attestation. *SocialCom/PASSAT* (pp. 768–775).
11. Goldwasser, S., Micali, S., & Rackoff, C. (1985). The knowledge complexity of interactive proof-systems (Extended Abstract). *STOC* (pp. 291–304).
12. Bitansky, N., Canetti, R., Chiesa, A., & Tromer, E. (2012). From extractable collision resistance to succinct non-interactive arguments of knowledge, and back again. *ITCS* (pp. 326–349).
13. Koch, K., Krenn, S., Pellegrino, D., Ramacher, S. (2021). Privacy-Preserving Analytics for Data Markets Using MPC. In: Friedewald, M., Schiffner, S., Krenn, S. (eds) *Privacy and Identity Management. Privacy and Identity 2020. IFIP Advances in Information and*

Communication Technology, vol 619. Springer, Cham. https://doi.org/10.1007/978-3-030-72465-8_13

14. Blaze, M., Bleumer, G., & Strauss, M. (1998). Divertible protocols and atomic proxy cryptography. *EUROCRYPT* (pp. 127–144).
15. Shamir, A. (1984) Identity-based cryptosystems and signature schemes. *CRYPTO* (pp. 47–53).
16. Archer, D. W., Bogdanov, D., Lindell, Y., Kamm, L., Nielsen, K., Pagter, J. I., Smart, N. P., & Wright, R. N. (2018). From keys to databases—real-world applications of secure multi-party computation. *The Computer Journal, 61*(12).
17. Mödersheim, S., Schlichtkrull, A., Wagner, G., More, S., & Alber, L. (2019) TPL: A trust policy language. *IFIP TM* (pp. 209–223).
18. Alber, L., Stefan, S., Mödersheim, S., & Schlichtkrull, A. (2022). Adapting the TPL trust policy language for a self-sovereign identity world. *Open Identity Summit*.
19. Alber, L., More, S., Mödersheim, S., & Schlichtkrull, A. (2021). Adapting the TPL Trust Policy Language for a Self-Sovereign Identity World. In: Roßagel, H., Schunck, C. H. & Mödersheim, S. (Hrsg.), *Open Identity Summit 2021*. Bonn: Gesellschaft für Informatik e.V.. (S. 107–118).
20. Kugler, L. (2018). The war over the value of personal data. *Communications of the ACM, 61,2*, 17–19.
21. Yeratziotis, A., Van Greunen, D., & Pottas, D. (2011). Recommendations for usable security in online health social networks. In *Pervasive Computing and Applications (ICPCA): 2011 6th International Conference IEEE*. Oct 220–226.
22. Daglish, D., & Archer, N. (2009). Electronic personal health record systems: A brief review of privacy, security, and architectural issues. privacy, security, trust and the management of e-Business. World Congress on December 2009.
23. European Data Protection Board. (2020). *Guidelines 05/2020 on consent under Regulation 2016/679*, 7–20.
24. Clifford, D., & Ausloos, J. (2017). Data protection and the role of fairness. CiTiP working Paper 29/2017, KU Leuven Centre for IT & IP Law, 11–20.
25. Lipworth, W. (2019). Real-world data to generate evidence about healthcare interventions. ABR11, 289–298 (2019). doi:https://doi.org/10.1007/s41649-019-00095-1. Accessed March 31, 2021from https://link.springer.com/article/10.1007/s41649-019-00095-1