# BROKERAGE AND MARKET PLATFORM FOR PERSONAL DATA

## *D7.1 Ethical and legal management report*

www.krakenh2020.eu

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

# D7.1 Ethical and legal management report

| | |
|---|---|
| **Grant agreement** | 871473 |
| **Work Package Leader** | KULEUVEN |
| **Author(s)** | Danaja Fabcic (KU Leuven) |
| **Contributors** | Jessica Schroers (KU Leuven), Wim Vandevelde (KU Leuven), Anton Vedder (KU Leuven), Sara Diez (ATOS) |
| **Reviewer(s)** | Stefan More (TUG), Ludovica Durst, Davide Zaccagnini (LYNKEUS) |
| **Version** | Final |
| **Due Date** | 31/07/2020 |
| **Submission Date** | 31/07/2020 |
| **Dissemination Level** | Public |

**Release History**

| Version | Date | Description | Released by |
|---|---|---|---|
| V0.1 | 13/01/2020 | ToC | Danaja Fabcic (KU Leuven) |
| V0.2 | 28/01/2020 | Detailed ToC | Danaja Fabcic (KU Leuven) |
| V0.3 | 03/02/2020 | ATOS input | Sara Diez (ATOS) |
| V0.4 | 26/06/2002 | Internal version | Danaja Fabcic (KU Leuven) |
| V0.5 | 20/07/2020 | Consolidated final draft | Danaja Fabcic (KU Leuven) |
| V0.5 | 21/07/2020 | ATOS input and review | Sara Diez (ATOS) |
| V0.5 | 27/07/2020 | Reviewed draft | Ludovica Durst and Davide Zaccagnini (Lynkeus) |
| V0.5 | 29/07/2020 | Reviewed draft | Stefan More (TUG) |
| V0.6 | 30/07/2020 | Final version after partner review | Danaja Fabcic (KU Leuven) |
| V1.0 | 31/07/2020 | Submitted version | Atos |

# Table of Contents

List of Tables ..... 5
List of Figures ..... 6
List of Acronyms ..... 7
Executive Summary ..... 8
1 Introduction ..... 9
1.1 The purpose of the deliverable ..... 9
1.2 The structure of the document ..... 10
1.3 Glossary adopted in this document ..... 10
2 Addressing legal and ethical challenges in KRAKEN research ..... 11
2.1 Legal sources for research ethics in KRAKEN ..... 11
2.2 Involvement of human participants in research ..... 13
2.2.1 Ethics of research with human participants ..... 14
2.2.2 Informed consent ..... 15
2.3 Use of personal data ..... 16
2.3.1 Data processing in KRAKEN ..... 16
2.3.2 Purpose limitation principle and secondary use of personal data ..... 17
2.4 Blockchain ..... 17
2.5 Privacy and data protection by design ..... 18
2.6 Residual ethical and legal challenges ..... 20
3 Ethics board ..... 22
4 Data protection impact assessment (DPIA) in the project ..... 23
4.1 When is it required to carry out a DPIA? ..... 23
4.2 Content of a DPIA ..... 24
4.3 DPIA and data use policy in the KRAKEN project ..... 25
5 Conclusion ..... 26
6 Bibliography ..... 27

# List of Tables

*Table 1: Addressing legal and ethical challenges in KRAKEN ..... 26*

# List of Figures

*Figure 1: Data protection/privacy by design requirement* ..... *20*

# List of Acronyms

| Acronym | Description |
|---|---|
| DoW | Description of Work |
| DPIA | Data protection impact assessment |
| EDPB (ex WP29) | European data protection board |
| EDPS | European data protection supervisor |
| GDPR | General data protection regulation (Regulation 2016/679) |
| KRAKEN | BroKeRage and MArKet platform for pErsoNal data, funded by Horizon 2020 programme under Grant Agreement no 837854 |
| PAB | Project advisory board |
| PIMS | Personal information management system |
| SSI | Self-sovereign identity |
| WP2 | Technical aspects and architecture specifications |
| WP7 | Ethical and legal compliance |
| WP8 | Ethics requirements |

# Executive Summary

Projects on personal information management systems (PIMS) like KRAKEN often bring legal and ethical challenges. Due to the nature of works, the challenges of research activities differ from those of system design and implementation. In this report, we address concerns arising from KRAKEN project research: involving human participants in trials, use of personal data, including sensitive personal data, and use of blockchain. We discuss the applicable legal and ethical framework and provide guidelines and procedures for facilitating adherence to relevant rules. We provide conclusions on lawful use of personal data in research, requirements for consent for human participants, and give guidelines on implementing privacy by design in the project research. Furthermore, the placement of personal data outside the blockchain is stressed. The document is primarily addressed to project partners; however, as the report will be made public, it can also serve as guidance and inspiration to similar projects.

This deliverable is part of KRAKEN's comprehensive effort in legal and ethical work on applicable legal framework (T2.1 Applicable legal framework and ethical principles and privacy metrics, T7.2 Ethical and Legal Analysis and Evaluation), WP8 (Ethical requirements), as well as the final legal evaluation (D7.3 Ethical and legal evaluation and recommendations).

# 1 Introduction

This deliverable is the first documented output of task T7.1 Ethical and Legal Management. This task runs throughout the project; it is led by KU Leuven as the legal experts and supported by other partners.

Task T7.1 involves the ethical and legal management of research activities throughout the project lifetime, including guidance on relevant research ethics related to the pilots; such as monitoring that informed consent and the necessary approvals are obtained. The work includes the production of documents related to the processing of personal data within research activities, for example informed consent forms and information sheets.

Further, this task identifies the need to conduct a data protection impact assessment, taking into account the use of new technologies and possible processing of personal data in accordance with the GDPR.[1] Conducting a data protection impact assessment will aid in the subsequent specification of legal requirements and broader issues.

*Relationship with other legal and ethical work in the project:*

The experience and the information obtained in this task will feed into the research and recommendations of the next task (T7.2 - Ethical and Legal Analysis and Evaluation), which runs through M3-36 of the project (February 2020 – November 2022). Even though D7.1 has a more compliance approach and focuses on the practical project research activities, the information obtained can be useful for the general analysis of requirements for the KRAKEN system (D7.2 Ethical and Legal Requirement Specification) and also for the evaluation of the project results (D7.3 Ethical and Legal Evaluation and Recommendations).

In terms of scope, this task differs from T2.1 Applicable legal framework and ethical principles and privacy metrics. While T2.1 identifies and analyses the legal and ethical framework applicable to the end-technology envisioned by KRAKEN, this task focuses on the research activities within KRAKEN itself. Both tasks have different aims, even though the frameworks identified in T2.1 may apply in a similar way.

The analysis conducted in this report builds on previous work and will facilitate future activities in WP8 – Ethics requirements.

This deliverable, D7.1, provides procedures and high levels guidelines to conduct project research activities including pilots in line with applicable ethical and legal principles. The legal analysis contained in this document complements practical implementation of ethical guidelines in WP7. The deliverable also contains the analysis whether a data protection impact assessment of the KRAKEN technology and surrounding application is necessary, as well as initial guidelines for a data protection impact assessment of the KRAKEN research activities, which will be further elaborated in D8.3 (due in M14 – February 2021).

## 1.1 The purpose of the deliverable

Establishing proper legal and ethical guidelines follows a two-fold objective:

- Firstly, guidelines serve as advice for research activities in KRAKEN, which establishes a link between this deliverable and WP8 – Ethics requirements and future work on legal and ethical aspects of the project. This includes addressing relevant requirements of research ethics,

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

establishing the ethics board as a single point of contact, laying down high-level measures to respect privacy by design etc.

- Secondly, this document will analyse whether there is a need to carry out a data protection impact assessment (DPIA – see art. 35 of the GDPR) in order to address risks to fundamental rights and freedoms, potentially posed by research with human participants and personal data.

## 1.2 The structure of the document

The report first addresses the legal and ethical challenges the project is likely to face in its research activities, such as involving human participants in pilots, processing of personal data, data protection in a blockchain context, implementation of privacy and data protection by design. The document outlines the consortium responses: risk management through specific measures and establishment of an ethics committee to oversee implementation.

Next, the data protection impact assessment is discussed: what is the role and nature of a DPIA and whether it could be necessary in a research project like KRAKEN.

## 1.3 Glossary adopted in this document

This report follows definitions laid down in article 4 of the General Data Protection Regulation (GDPR), as well as other applicable legal instruments.

***Personal data*** means any information relating to an identified or identifiable natural person ('data subject').

***Data subject*** is an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

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

***Data controller*** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

***Data processor*** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

# 2 Addressing legal and ethical challenges in KRAKEN research

KRAKEN is an EU project, funded by the Horizon 2020 Framework. The Horizon 2020 Framework was established by Regulation no. 1291/2013/EU.[2] The rules applicable to participation and dissemination in Horizon 2020 are set out in Regulation 1290/2013/EU.[3]

Article 19 of Regulation 1291/2013 sets out the ethical principles with which all actors in Horizon 2020 projects need to comply: "All research and innovation activities carried out under Horizon 2020 need to comply with ethical principles set out in this article and with relevant legislation. Particular attention is paid to the principle of proportionality, the right to privacy, the right to protection of personal data, the right to the physical and mental integrity of a person, the right to non-discrimination and the right to ensure high levels of human health protection. Research and innovation must be focused exclusively on civil application."

The main ethical concerns of the project relate to the involvement of human participants in the project's research and the handling of personal data.

## 2.1 Legal sources for research ethics in KRAKEN

The legal framework for managing legal and ethical challenges of KRAKEN is based on European legal framework for ICT research in H2020 projects: Commission Guidelines, the General Data Protection Regulation (GDPR),[4] and expert opinions, such as the recently adopted EDPS opinion on data protection in scientific research.[5]

***The GDPR applies to processing of personal data***. These notions are defined in Art. 4(1) and (2):

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

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

Its scope of application is therefore relatively broad; the rules apply in any context that involves processing personal data, including academic and industrial research, testing, validation, etc.

[2] Regulation (EU) No 1291/2013 of the European Parliament and of the Council of 11 December 2013 establishing Horizon 2020 - the Framework Programme for Research and Innovation (2014-2020) and repealing Decision No 1982/2006/EC.

[3] Regulation (EU) No 1290/2013 of the European Parliament and of the Council of 11 December 2013 laying down the rules for participation and dissemination in "Horizon 2020 - the Framework Programme for Research and Innovation (2014-2020)" and repealing Regulation (EC) No 1906/2006.

[4] See fn. 1.

[5] European Data Protection Supervisor, A Preliminary Opinion on data protection and scientific research.

***Research ethics in Horizon 2020*** are governed by rules laid down by the Commission in two relevant sets of guidelines: first, a general guide on completing ethics self-assessment,[6] which cover overarching ethical issues in Horizon 2020 projects, its chapters 2 (Human beings) and 4 (Personal data) are the most relevant for projects like KRAKEN. The second document is specialized on ethics and data protection in projects.[7]

An important requirement of the guidelines is obtaining *informed consent* – however, it appears to be different from the GDPR consent requirements, and the connection between the two seems unclear. In some cases pre-existing consent is not appropriate legal grounds for data processing in research projects, since specific legal basis for processing might have to be obtained. Under the wording of GDPR's Recital 50, it was not clear whether it is necessary to obtain new legal grounds for secondary use of personal data. In the recently published Preliminary opinion,[8] which is still open for comments and feedback, some more holistic guidance is offered: where consent (in the GDPR sense) is not appropriate as a legal basis and other legal basis is necessary, informed consent (as a human research participant) could still serve as an 'appropriate safeguard' of the rights of the data subject. The opinion suggests using *tiered and dynamic consent* to overcome the hurdles of legal uncertainty. This fits with the approach of KRAKEN platform, which enables data subjects to set specific data sharing options and give or withdraw consent accordingly.

Managing legal and ethical risks in KRAKEN is based on three main principles, identified in Section 5 of the DoW:

1. Data protection and privacy by design

KRAKEN researchers as well as the final KRAKEN platform will process personal data to some extent. Given the importance of protecting personal data, the aspects of data security, data protection and privacy will be taken into account throughout the engineering and design process, as well as during testing and evaluation phases. Measures and technologies such as strong end-to-end encryption, personal information management systems (PIMS), self-sovereign identity (SSI) and blockchain will be used in order to allow the user to retain control over personal data and credentials.

2. Improved informed consent tools

Obtaining informed consent is an important tenet for all KRAKEN research activities. The high legal value of consent has been called "moral magic"; for example, consent "turns ... a kidnapping into a Sunday drive, a battery into a football tackle, a theft into a gift, and a trespass into a dinner party".[9] Consent must be freely given, specific and informed, and must represent an unambiguous indication of the data subject's wishes. In KRAKEN, users of the platform will be able to manage their consent and data sharing options through dedicated mobile and web-based interfaces.

3. Data minimization and purpose limitation principles

[6] Horizon 2020 Programme Guidance: How to complete your ethics self-assessment, European Commission, February 2019.
[7] Ethics and data protection, European Commission, November 2018.
[8] European Data Protection Supervisor, A Preliminary Opinion on data protection and scientific research.
[9] Meg Leta Jones, 'The Right to a Human in the Loop: Political Constructions of Computer Automation and Personhood' (2017) 47 Social Studies of Science 216.

Data minimization, also referred to as the data adequacy principle,[10] means that personal data used in the research must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. Only directly relevant and necessary data are allowed to be processed and kept no longer than necessary to achieve a specific goal. This means that if an objective/a goal can be reached without processing personal data, then using personal data would go against the data minimization principle. In KRAKEN research, synthetic data will be used for the platform implementation.

Purpose specification principle means that personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. This principle establishes 'the boundaries within which personal data collected for a given purpose may be processed and may be put to further use.'[11]

In a research setting like KRAKEN, the GDPR provides for a lighter-touch regime.

- According to art. 5(1)(b) of the GDPR, further processing of already collected personal data for scientific research purposes is not considered to be incompatible with the initial purposes. However, the EDPS Opinion[12] suggests that, despite the wording of Recital 50, secondary uses of personal data may still require a legitimate ground under Article 6 or Article 9. Therefore, KRAKEN partners will endeavor to obtain valid legal grounds for processing, where applicable.
- Art. 89 provides for safeguards in the context of processing of personal data for research purposes. These include technical and organisational measures to ensure data minimization, including pseudonymisation or depersonalization (de-identification) of personal data as long as those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects.

In the proposal phase, two different ethical areas were identified – involvement of human participants in research and use of personal data. They are addressed in this section together with relevant associated challenges.

## 2.2 Involvement of human participants in research

In KRAKEN pilots, humans will be involved, since the aim of the project is to validate the platform by real-life users. In the **education scenario**, university students will have the opportunity to test the process of issuing verifiable credentials. In the **health scenario**, participants will be enrolled from the general, unselected population on a voluntary basis through standard communication channels (website, social media, newsletter, …). The project does not intend to enrol children and/or adults unable to give informed consent and/or individuals belonging to other vulnerable groups.

The question of involving participants is dealt with in-depth within WP8: in order to meet the additional ethics requirements, *informed consent forms and information sheets* pursuant to articles 13-14 of the GDPR and Commission's ethics guidelines, as well as *relevant approvals of ethics committees and/or competent authorities* are submitted as deliverables – D8.1 and D8.5, respectively. Moreover, *an ethics board* will oversee the process of collecting sensitive data, as described in report no. D8.4.

---

[10] Information Commissioner's Office, Principle C: Data minimisation <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation/>

[11] Article 29 Working Party, Opinion on Purpose Limitation

[12] European Data Protection Supervisor, A Preliminary Opinion on data protection and scientific research, point 6.7.

### 2.2.1 Ethics of research with human participants

Respecting participants' dignity is an important tenet of ethical research with humans. In this subsection we explore basic ideas of moral philosophy that are relevant to KRAKEN research activities, especially the principles of non-discrimination, fair treatment, beneficence and non-maleficence, and respect for human dignity. Throughout project research activities, the KRAKEN partners will use ethically sound scientific methods for correct interpretation of research results, dissemination and publication of results in order to minimise ethical risks to participants.

Research must be carried out respecting the principle of ***non-discrimination***. Discrimination is the unequal or unfair treatment of another person on the basis of their personal characteristics. Currently, research in KRAKEN does not seem to pose discrimination risks: participants will be chosen without discriminatory criteria, no different treatment of any group/individual is foreseen. If necessary, to ensure non-discrimination in research, inclusion/exclusion criteria for participants will be further defined in WP5 works as part of pilot execution.

The notion of ***autonomy*** is based on principle of respect for persons; in research, that means asking informed consent from the participants. The notion of informed consent is based on two premises: the *prudent person rule* meaning the person understands the risks and benefits as well as procedures pertaining to research, and non-concealment of any relevant information that may lead the person to refuse their participation in a study (referred to as "subjective substantial disclosure"). Participants in KRAKEN pilots will be well briefed about relevant procedures, risks and benefits in advance, and they will always have the option to contact pilot leaders for more information. The right to withdraw from research is equally important to giving informed consent: pilot participants will have the option to withdraw at any time.

***Beneficence*** means we must do good, and act in the participant's interests, other things being equal. Hence, maximising risks and minimising harms so that technology can benefit humanity is an important tenet of research ethics. Inversely, the principle of ***non-maleficence*** means, other things being equal, we must refrain from doing harm or going against the participants' interests. The principle of ***justice*** requires fair distribution of goods and services. The underlying objective of PIMS is to give back control over personal information to data subjects instead of leaving the power in the hands of big technological corporations. Specific participants' interests in research and pilots will duly be taken into account in WP5 as part of user stories, where typical interests will be translated into more specific terms. In KRAKEN pilots, the risk of injustice is mild, since the same platform will be tested by participants, and their feedback taken into account to address possible injustices and shortcomings.[13]

***Fair treatment of participants*** is linked to protecting their informational privacy, transparent disclosure policies and provision of quality information relevant to pilots so that the participants can freely decide if they wish to participate. That also includes the right to withdraw their participation from the research.[14]

PIMS are important means of empowerment of individuals in managing all aspects of their personal data: the objectives of PIMS and underlying technologies, such as SSI, are therefore aligned with the principle of fair treatment. These systems also have an impact on *network effect*, which means that the value of network increases with the number of users joining the network. [15] A critical mass of individual users as well as organisations consuming those individuals' data is required for the network to function. However, it may lead to problems related to ***lock in and lock out of users***: if switching from

[13] Beauchamp, Tom L, and Childress, James F. Principles of Biomedical Ethics. 7th ed. New York: Oxford UP, 2013.
[14] Iphofen, Ron. Ethical Decision Making in Social Research: A Practical Guide. Basingstoke: Palgrave, 2011. Bhattacherjee A, Social Science Research: Principles, Methods, and Practices. University of South Florida text book collections 2012.
[15] Network effect is the most obvious in social networks, where more users also mean more advertising revenue.

one network provider to another has high transaction costs, users feel they are locked in with that system; on the other hand, those without an access to the network, may not have access to important services, such as eGovernment and healthcare.[16]

We do not foresee large lock in/lock out effects of the research in KRAKEN due to its limited scope. The platform will be developed and evaluated in two pilot settings with a relatively small participant base and no access to essential services. Moreover, the concepts of SSI/PIMS aim to address the problems of lock in and lock out by empowering the participant to take control of their data.

***Respect for personal and social identity*** is another important principle. Identity management is based on complementary aspects of memory and forgetting. The internet never forgets – we may well be coming into an unforgiving culture, in which it is easy to shame someone based on their employment history, social status and surveillance policies. The concepts of personal identity, social identity and self-perception are thus tightly intertwined with technological developments in identity management community. The right to be forgotten (right to erasure under art. 17 of the GDPR) combined with a comprehensive PIMS may well be an answer to the advent of shaming culture.[17]

### 2.2.2 Informed consent

Obtaining valid informed consent from participants is an important obligation from perspective of legal framework on data protection as well as in the context of research ethics. The two notions differ somewhat due to different relevant frameworks and as we explained in D8.1, there is little clarity on their relationship. Here we summarise the findings of applicable frameworks for informed consent in the GDPR and in research ethics and their implications for KRAKEN research activities.

**Consent in GDPR**

GDPR imposes strict requirements for valid consent: processing of personal data is legitimate only insofar valid legal basis exists, and **consent** to the processing of personal data **for one or more specific purposes** can represent such legal basis.[18]

To be valid under the GDPR, consent must (cumulatively) fulfil the following requirements: be freely given; specific; informed; unambiguous; be given by a statement or by clear affirmative action.[19] However, in scientific research determining the purposes ex ante might be difficult due to the inherent nature of research. This is fully recognized by the GDPR's Recital 33. Since it is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection, data subjects should be allowed to give their consent to certain areas of scientific research when in keeping with recognised ethical standards for scientific research. Data subjects should have the opportunity to give their consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose.

Art. 7 lays down detailed conditions for valid consent:

- The controller must be able to demonstrate that the data subject has consented to processing of his or her personal data;
- The request for consent shall be presented in a manner clearly distinguishable from any other matters discussed in the context of a written declaration; it must be requested in an intelligible and easily accessible form, using clear and plain language.

[16] Schroers, Jessica; 2019. I have a Facebook account, therefore I am – authentication with social networks. International Review of Law, Computers and Technology; 2019; Vol. 32; iss. 2; pp. 211 - 223
[17] European Group of Experts, ICT, 2012 p. 41.
[18] Art. 6(1)(a) of the GDPR.
[19] Art. 4(11) of the GDPR.

- The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.
- It is important that consent be freely given. When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

**Informed consent in research ethics framework of Horizon 2020**

In Horizon 2020 projects, rules that are more specific apply. These rules are contained in the ethics self-assessment manual, last updated by the Commission in February 2019.[20] Its section 2 refers to research with humans and sub-section 2.3 with conditions for informed consent.

More specifically, participants must be given an informed consent form and detailed information sheets that:

- Are written in a language and in terms participants can fully understand
- Describe the aims, methods and implications of the research, the nature of the participation and any benefits, risks or discomfort that might ensue
- Explicitly state that participation is voluntary and that anyone has the right to refuse to participate and to withdraw their participation, samples or data at any time —without any consequences

Moreover, potential participants have to understand the information fully and must not feel pressured or coerced into giving consent.

Consent requirements were fully considered and integrated in the design of informed consent forms and information sheets, which were released in D8.1 in M6 (June 2020) of the project. In order to ensure fair treatment of participants, they will be recruited on a voluntary basis, appraised of their rights under applicable legal instruments, and they will have the option to contact partners, responsible for carrying out the trials. The procedure is described in informed consents forms, which will be given out before the pilots start. Once the candidates have received all relevant information, they will be free to decide whether they wish to enroll in the pilots. In other words, they will decide whether to give their consent.

## 2.3 Use of personal data

### 2.3.1 Data processing in KRAKEN

As explained in section 2.1, GDPR applies to processing of personal data. “Processing” is understood widely by the Regulation: it means *any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.*

[20] European Commission, Horizon 2020 Programme Guidance: How to complete your ethics self-assessment.

There are two options: personal data can be obtained directly from the data subject ("primary processing") or otherwise, from other sources ("secondary processing", also called reuse of personal data).

Report D8.6 describes the data use policies in KRAKEN. At the time of writing this report (July 2020), the partners have not yet decided whether or how (identifiable) personal data will be used in the project pilots. While the platform will initially be developed and tested using synthetic/non-personal data, personal data might be processed in the context of pilot validation.

### 2.3.2 Purpose limitation principle and secondary use of personal data

**Purpose limitation** means that data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.[21] This principle establishes 'the boundaries within which personal data collected for a given purpose may be processed and may be put to further use.'[22] It consists of two building blocks:

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

Specific purpose means that the purpose must be 'sufficiently defined to enable the implementation of any necessary data protection safeguards and to delimit the scope of the processing operation'. An explicit purpose is one that is 'sufficiently unambiguous and clearly expressed'. The notion of legitimate purpose goes beyond the scope of privacy rules and requirement of legal grounds for data processing.[23]

Purpose specification is related to concepts such as data transparency (visibility of purpose), predictability of data processing and user control, i.e. giving data subjects certain rights regarding the collected data.[24]

Sometimes, data may be further processed for different purposes for which original consent had not been given (*data reuse*). On principle, further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1) of the GDPR, not be considered to be incompatible with the initial purposes[25]. Article 89(1) provides that it is only possible if appropriate safeguards, such as pseudonimisation and access controls, are put in place. Moreover, WP29 points out that it should be ensured data is then not reused to make decisions about any single individual.[26] The EDPS, following WP29's argument, further states that the principles of purpose limitation and lawfulness should be understood cumulatively: reusing data requires a new legal basis, even if done so for scientific purposes.[27]

Opinions and recommendations are of course non-binding legal texts. Nevertheless, in the absence of clear diction in the statute, they should be adhered to wherever possible. Therefore, in KRAKEN project, project partners shall endeavour to obtain valid consent to use personal data for research purpose, whenever that is feasible.

## 2.4 Blockchain

The KRAKEN project will use a blockchain infrastructure for data access control integrated with a Self-Sovereign Identity (SSI) system. Blockchain has often been considered to have a difficult relationship

[21] Article 5(1)b of the GDPR.
[22] Article 29 Working Party, Opinion 03/2013 on Purpose Limitation, p. 4.
[23] Article 29 Working Party, Opinion 03/2013 on Purpose Limitation, p. 12.
[24] Article 29 Working Party, Opinion 03/2013 on Purpose Limitation, p. 13-14.
[25] Article 5(1)b of the GDPR.
[26] Article 29 Working Party, Opinion 03/2013 on Purpose Limitation, p. 33.
[27] See footnote 12.

with data protection legislation.[28] Blockchain can be described as "a shared and synchronised digital database that is maintained by a consensus algorithm and stored on multiple nodes (computers that store a local version of the database). Blockchains are designed to achieve resilience through replication, meaning that there are often many parties involved in the maintenance of these databases. Each node stores an integral copy of the database and can independently update the database. In such systems, data is collected, stored and processed in a decentralised manner. Furthermore, blockchains are append-only ledgers to which data can be added but removed only in extraordinary circumstances."[29]

The main reason that blockchain is considered to be on difficult terms with data protection legislation is the data integrity, which is achieved by hashes and often a work intensive consensus protocol, due to which information stored on the blockchain cannot simply be changed or erased. This is at odds with some data protection principles and data subject rights, such as the principle of data minimization, storage limitation, right to rectification, right to erasure, right to restriction of processing and right to object. For this reason no personal data will be stored on the blockchain, following the successful implementation strategy of the MyHealth-MyData project on which the KRAKEN platform will be built. This is also the approach taken by SSI. One issue which is still discussed in the academic literature is whether public keys could be considered personal data. This discussion and the application of the GDPR (and the eIDAS Regulation)[30] to SSI will be further analysed in D7.2 Ethical and Legal Requirement Specification.

## 2.5 Privacy and data protection by design

The GDPR sets out a stricter regime for data protection and data security than the previously applicable Directive 95/46/EC[31] by introducing the concept of data protection by design and by default (hereafter: data protection by design). Data protection by design requires that data protection be included from the onset of the designing of systems, rather than as a later addition.

Data protection by default is among the general obligations of the controller. One of its purposes is to contribute to the principle of accountability, under which the data controller must be able to show

[28] See e.g. Michèle Finck, 'Blockchains and Data Protection in the European Union' 32; Michèle Finck, 'Blockchain and the General Data Protection Regulation - Can Distributed Ledgers Be Squared with European Data Protection Law?' (2019) <http://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf> accessed 8 December 2019; Christopher Kuner and others, 'Blockchain versus Data Protection' (2018) 8 International Data Privacy Law 103; Philipp Quiel, 'Blockchain-Technologie im Fokus von Art. 8 GRC und DS-GVO: Ein Zwiespalt zwischen Innovation und unionalem Datenschutzrecht?' (2018) 42 Datenschutz und Datensicherheit - DuD 566; Dalmacio V Posadas, 'The Internet of Things: The GDPR and the Blockchain May Be Incompatible' (2018) 21 Journal of Internet Law 12; Ninja Marnau, 'Die Blockchain im Spannungsfeld der Grundsätze der Datenschutzgrundverordnung' in Eibl M and M Gaedke, (eds), Lecture Notes in Informatics (LNI) (Gesellschaft für Informatik); Luis-Daniel Ibáñez, Kieron O'Hara and Elena Simperl, 'On Blockchains and the General Data Protection Regulation' Report for EU Blockchain Forum <https://www.eublockchainforum.eu/sites/default/files/research-paper/blockchains-general-data_4.pdf?width=1024&height=800&iframe=true> accessed 3 June 2019.

[29] Finck, 'Blockchain and the General Data Protection Regulation - Can Distributed Ledgers Be Squared with European Data Protection Law?'.

[30] 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

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

compliance with the requirements of the GDPR. Measures undertaken should be in line with the current state of the art and adopted with the aim of complying with the data controllers' obligations.[32]

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

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

The specific obligation for the data controller is therefore to adopt measures, which implement data protection principles: lawfulness and fairness, data minimisation, purpose limitation, storage limitation and integrity and confidentiality.

GDPR suggests the adoption of the following measures, which contribute to privacy by design: minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing and enabling the controller to create and improve security features.[33]

In May 2018, the EDPS (European Data Protection Supervisor) issued a Preliminary Opinion on Privacy by Design, aiming to provide guidance to controllers and processors for the implementation of the principle.[34] The Preliminary Opinion further describes the key aspects of Data Protection by Design and outlines three possible steps for the operationalisation thereof. These are:

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

The key is therefore to focus on both legal compliance and on risks from computer engineering point-of-view. It is especially important that privacy by design is not understood as solely an IT solution to the privacy risks, but also in a processual manner, encompassing compliance, computer engineering, business and organisational processes.[35]

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

[32] See Recital 78 of the GDPR.
[33] Recital 78 of the GDPR.
[34] European Data Protection Supervisor, Opinion 5/2018 - Preliminary Opinion on privacy by design
[35] Regulating privacy by design (privacy enhancing technologies (Technology: Transforming the Regulatory Endeavor, Rubinstein, Ira S., Berkeley Technology Law Journal, Summer, 2011, Vol. 26 (3).

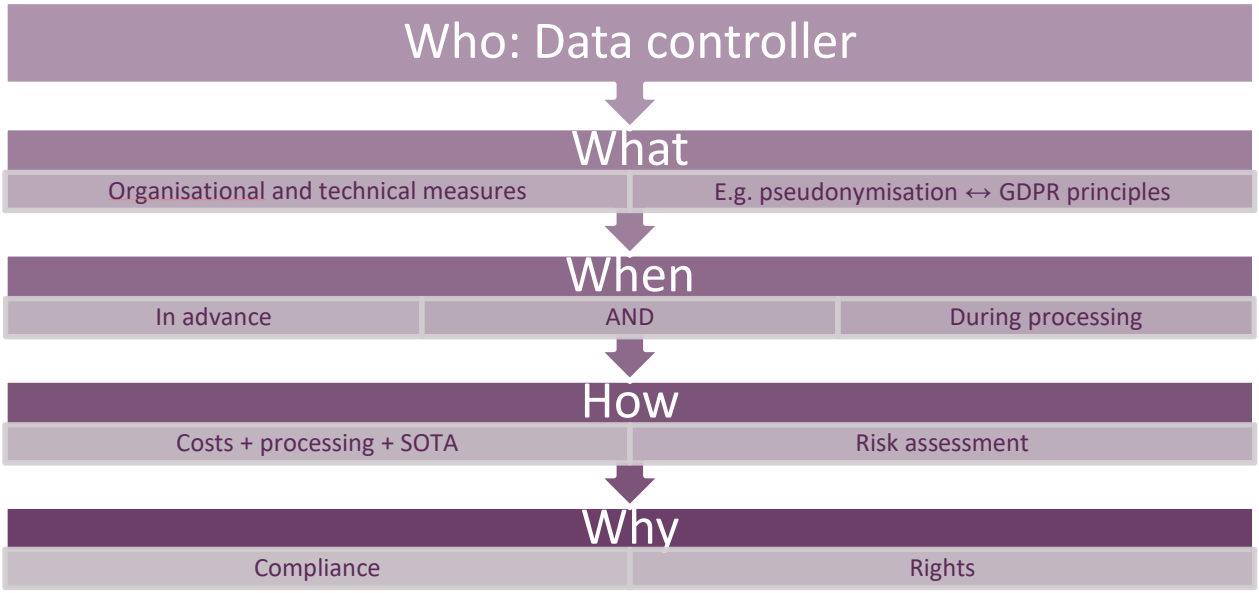


**Figure 1: Data protection/privacy by design requirement**

Legal challenges in the KRAKEN project relate to privacy and data protection by design with regard to the research trials and eventual implementation of the resulting technologies due to information sharing in the context of personal information management systems (PIMS). The approach taken by partners is described in D8.6 and is founded on continuous interaction between legal and technical experts since the beginning of the project. It is based on elementary principles of data quality, accountability and technical and organisational measures against re-identification and reverse engineering.

Data used within the project will be pseudonymised and/or anonymised as soon as possible, which is specifically mentioned in the GDPR as a data protection by design measure. Pseudonymisation includes the encryption of data, which is a specific focus point of the KRAKEN project and will be addressed in WP4. Cryptographic work includes the provision of cryptographic tools for end-to-end secure data sharing, to provide confidentiality of privacy-sensitive data while performing data analysis and to ensure secure implementation of crypto technologies. For the privacy-preserving data analysis schemes based on functional encryption, homomorphic encryption and secure multi-party computation will be analysed.

To comply with data minimisation, the personal data will remain under the data subjects' control and on their own devices as much as possible; only metadata will be stored by the platform.

Moreover, transparency measures will be implemented, such as the advanced consent solution, which enables an easy and granular way to give and revoke consent, and the possible inclusion of privacy metrics in the system.

## 2.6 Residual ethical and legal challenges

How to deal with new ethical and legal challenges that might occur unexpectedly?

In the KRAKEN project, all the partners endeavour to address any legal and ethical risks in continuous interaction with each other, especially making sure the ethical experts of KU Leuven (and if necessary, the project ethics board) are involved. Follow-up during regular and ad-hoc telcos as well as by email is the starting point for addressing any issues and will be used to the extent possible given budget and travel constraints (especially since the project started during a pandemic). The project risk registry may

also be used to manage ethical risks. Moreover, if necessary, new risks can be discussed in face-to-face meetings and consultations, for example during a consortium meeting.

# 3 Ethics board

According to Section 5 of the DoW, and Requirement No. 6 – GEN, an ethics board is appointed to oversee most sensitive ethical and legal aspects of KRAKEN research.[36] The board comprises one person from each involved partner, as well as a member of the project advisory board (PAB). The names of members of the ethics board are contained in the D8.4.The board will be consulted regarding the use of sensitive personal data – defined as "special categories of personal data " in art. 9(1) of the GDPR: these are "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership; genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation". Their processing is prohibited, unless any of the ten legal grounds from art. 9(2) are provided.

In the KRAKEN medical and well-being use-case, personal data on health status will on principle **not be processed**. Nevertheless, to meet the Requirement No. 6 – GEN, the ethics board will oversee the implementation of the use-case and issue a screening report in M15 (February 2021) on how ethical issues were handled.

[36] More information on the composition and role of the ethics board can be found in D8.4 Requirement No. 6 – GEN.

# 4 Data protection impact assessment (DPIA) in the project

A **data protection impact assessment/privacy impact assessment** (DPIA/PIA) is one of the starting points for the data controllers to apply the requirements of privacy by design to the actual technology. A DPIA is carried out as a part of the design phase. It is meant to identify the stakeholders (and consult with them), the risks, solutions and recommendations, implement those recommendations as well as provide for review, audit and accountability measures.[37]

## 4.1 When is it required to carry out a DPIA?

Carrying out a DPIA is required in three situations:

1) The data controller is explicitly required to do so by the GDPR in the following cases:
   a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
   b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or
   c) a systematic monitoring of a publicly accessible area on a large scale.[38]
2) If the processing activity is on the list, published by the national supervisory authority.[39]
3) If the processing is likely to result in a high risk to the rights and freedoms of natural persons, especially if new technologies are used.[40]

The first and second instance are clear in their wording. Given KRAKEN's research objectives and use of data, ***we do not foresee its falling under either of those two provisions***.

However, the third instance of obligatory DPIA is worth examining, due to its broad wording. ***High risk*** is the deciding criterion for necessity of a DPIA under the third instance. When identifying high risk, the following criteria must be considered, although this list is not definitive:[41]

1) Evaluation or scoring, including profiling and predicting,
2) Automated decision-making with legal or similar significant effects,
3) Systematic monitoring,
4) Processing of sensitive data,[42]
5) Data processed on a large scale, 'large scale' depending on

[37] ENISA, Privacy and Data protection by design, January 2015, p. 12.
[38] Article 35(3) of the GDPR.
[39] Article 35(4) of the GDPR.
[40] Article 35(1) of the GDPR.
[41] National data protection authorities may designate lists of processing activities for which a DPIA is (not) necessary – article 35(4,5) of the GDPR.
[42] According to Art. 9(1) GDPR, Sensitive data is personal data revealing *racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership,* and the processing of *genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation*.

a) The number of data subjects concerned, either as a specific number or as a proportion of the relevant population,
b) The volume of data and/or the range of different data items being processed,
c) The duration, or permanence, of the data processing activity,
d) The geographical extent of the processing activity;

6) Combined or matched datasets,
7) Data concerning subjects who are vulnerable due to power imbalance between them and the data controller, e.g. children, employees, patients, asylum seekers …,
8) Innovative use or applying technological or organisational solutions, such as combining use of finger print and face recognition for improved physical access control, or certain applications of internet of things,
9) Data transfers to non-EU countries,[43]
10) Processing that by itself prevents data subjects from exercising a right or using a service or a contract.[44]

If at least two of the above criteria are met, the processing is likely to result in a high risk and there is a need to carry out a DPIA. If fewer than two criteria are met, the processing is deemed to be low-risk and there is no need for a DPIA.[45]

The only criterion potentially relevant during the KRAKEN research phase is processing of sensitive (health) data in the health use-case. However, the project partners will be using fake, synthetic data to develop and test the platform, and potentially use real sensitive personal data only for pilot evaluation phase. Using sensitive personal data will not be carried out on a large scale in the sense of art. 35. Based on the information available in the current stage of development, this type of processing ***does not represent a high risk*** as understood by art. 35 and the guidelines. Nevertheless, should it become necessary to use real personal data for testing and implementation purposes, the partners will re-evaluate whether high risks could manifest in project research activities.

In a post-project scenario, the need to carry out a DPIA will depend largely on the product's end-use. Due to PIMS' inherent characteristics, the criteria of use of combined or matched datasets and using data in innovative ways or applying technological or organisational solutions might well be relevant. While the EDPS largely sees PIMS as a compliance opportunity and a means of enhancing individuals' data protection[46] and the research carried out in KRAKEN is limited in scope, eventual end users may need to conduct a DPIA to understand data protection risks and address them accordingly.

## 4.2 Content of a DPIA

The DPIA assesses the impact of the envisaged processing operations on the protection of personal data for a single operation or a set of similar processing operations that present similar high risks. It takes into account the nature, scope, context and purposes of the processing. It focuses at least on:

- A systematic description of the envisaged processing operations and the purposes of the processing;

[43] This situation was eventually dropped in the revised guidelines.

[44] Working Party 29, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, wp248 rev.01, p. 8-9.

[45] Idem.

[46] EDPS, Opinion on Personal Information Management Systems: Towards more user empowerment in managing and processing personal data, October 2016

- 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;
- the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the GDPR taking into account the rights and legitimate interests of data subjects and other persons concerned.[47]

## 4.3 DPIA and data use policy in the KRAKEN project

As we have seen, a DPIA is most likely not required for KRAKEN project research activities, since it does not fall under any of the situations envisioned in art. 35, nor is the processing likely to meet the high-risk criterion. The use of personal data in the project research is not yet fully defined by pilot owners; the implications have been thoroughly discussed in section 2 of this report, as well as relevant deliverables in WP8.

However, once the project is over and the KRAKEN platform is used by individuals - data subjects – it might become necessary to carry out a corresponding DPIA. The understanding of necessity will largely depend on manner of application; for example, patients using it to manage their health data might carry higher data protection risks than its use for purely household activities (e.g. sharing holiday photos among family members). In the current stage of the project, it is not yet possible to predict future use of the resulting platform. In D8.3 (POPD – Requirement no. 5), an in-depth analysis on ethics risks of data processing activities will be carried out in order to evaluate the risks within the context of project research and the necessity to address them with a DPIA. If necessary, the DPIA for KRAKEN use-cases (education and health) will be carried out. In that case, the assessment can serve as the basis for DPIA by future adopters, considering legal recommendations stemming from D7.3 Ethical and Legal Evaluation and Recommendations.

[47] Article 35(7) of the GDPR.

# 5 Conclusion

This report provides procedures and guidelines to facilitate conducting KRAKEN project research, including pilots, in line with applicable legal and ethical frameworks. Applicable principles come from the General Data Protection Regulation (GDPR), Commission's guidelines on research ethics, and expert opinions. Main legal and ethical concerns in the project stem from the involvement of human participants in the pilots, processing of personal data and use of blockchain. Implementation of privacy and data protection by design is also addressed. Risk mitigation measures are addressed alongside challenges throughout the document, and can be summarised in a table:

| Source of legal and ethical concern | Proposed action | Relevant deliverables |
|---|---|---|
| Involvement of human participants in pilots | Informed consent procedures | D8.1 |
| Processing of personal data | Data use policy<br>Approvals by relevant bodies<br>Tiered consent (consent settings)<br>Data protection by design approach | D7.1, D8.6<br>D8.5<br>D8.1, privacy metrics in WP2<br>D7.1, D8.6 |
| Potential use of sensitive data in health pilot | Ethics committee | D8.4 |
| Immutability of blockchain | No personal data will be stored on blockchain | Technical works in WP2-3<br>D7.2 |
| Residual challenges | Continuous and ad-hoc interaction between partners through email, telcos and in-person meetings<br>Risk management process | Internal project reports |

**Table 1: Addressing legal and ethical challenges in KRAKEN**

The findings from this deliverable will be taken into consideration throughout the project research works in the areas identified. A final legal evaluation will be provided in D7.3 Ethical and Legal Evaluation and Recommendations, due in the final month of the project (December 2022).

# 6 Bibliography

Article 29 Working Party, Opinion 03/2013 on Purpose Limitation

Article 29 Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, wp248 rev.01

Beauchamp, Tom L, and Childress, James F. Principles of Biomedical Ethics. 7th ed. New York: Oxford UP, 2013.

Bhattacherjee A, Social Science Research: Principles, Methods, and Practices. University of South Florida text book collections 2012.

ENISA – European Agency for cybersecurity, Privacy and data protection by design, January 2015

European Commission, Horizon 2020 Programme Guidance: How to complete your ethics self-assessment, February 2019

European Commission, Ethics and data protection, November 2018

European Data Protection Supervisor, Preliminary Opinion on data protection and scientific research, January 2020

EDPS, Opinion 09/2016 on Personal Information Management Systems: Towards more user empowerment in managing and processing personal data, October 2016

European Data Protection Supervisor, Opinion 5/2018 - Preliminary Opinion on privacy by design, May 2018

Finck M, 'Blockchain and the General Data Protection Regulation - Can Distributed Ledgers Be Squared with European Data Protection Law?' (2019) <http://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf> accessed 8 December 2019

Finck M, 'Blockchains and Data Protection in the European Union' 32

Ibáñez L-D, O'Hara K and Simperl E, 'On Blockchains and the General Data Protection Regulation' Report for EU Blockchain Forum <https://www.eublockchainforum.eu/sites/default/files/research-paper/blockchains-general-data_4.pdf?width=1024&height=800&iframe=true> accessed 3 June 2019

Information Commissioner's Office, Principle C: Data minimisation <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation/>

Iphofen, Ron. Ethical Decision Making in Social Research: A Practical Guide. Basingstoke: Palgrave, 2011. Print.

Jones ML, 'The Right to a Human in the Loop: Political Constructions of Computer Automation and Personhood' (2017) 47 Social Studies of Science 216

KRAKEN D2.1 Ethical and Legal Framework Report (due August 2020)

KRAKEN D7.2 Ethical and legal requirement specification (due September 2020)

KRAKEN D8.1 H - Requirement No. 2 (submitted May 2020)

KRAKEN D8.4 GEN - Requirement No. 6 (submitted February 2020)

KRAKEN D8.5 H - Requirement No. 7 (submitted May 2020)

KRAKEN D8.6 POPD - Requirement No. 8 (submitted May 2020)

Kuner C and others, ‘Blockchain versus Data Protection’ (2018) 8 International Data Privacy Law 103

Marnau N, ‘Die Blockchain im Spannungsfeld der Grundsätze der Datenschutzgrundverordnung’ in Eibl M and M Gaedke, (eds), Lecture Notes in Informatics (LNI) (Gesellschaft für Informatik)

Posadas DV, ‘The Internet of Things: The GDPR and the Blockchain May Be Incompatible’ (2018) 21 Journal of Internet Law 12

Quiel P, ‘Blockchain-Technologie im Fokus von Art. 8 GRC und DS-GVO: Ein Zwiespalt zwischen Innovation und unionalem Datenschutzrecht?’ (2018) 42 Datenschutz und Datensicherheit - DuD 566

Regulation (EU) No 1290/2013 of the European Parliament and of the Council of 11 December 2013 laying down the rules for participation and dissemination in "Horizon 2020 - the Framework Programme for Research and Innovation (2014-2020)" and repealing Regulation (EC) No 1906/2006.

Regulation (EU) No 1291/2013 of the European Parliament and of the Council of 11 December 2013 establishing Horizon 2020 - the Framework Programme for Research and Innovation (2014-2020) and repealing Decision No 1982/2006/EC.

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

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)

Rubinstein, IS, 'Regulating privacy by design (privacy enhancing technologies (Technology: Transforming the Regulatory Endeavor)' (2011) Berkeley Technology Law Journal, Vol. 26 (3)

Schroers, Jessica; 2019. I have a Facebook account, therefore I am – authentication with social networks. International Review of Law, Computers and Technology; 2019; Vol. 32; iss. 2; pp. 211 - 223


Atos

FONDAZIONE BRUNO KESSLER

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY

sic

LYNKEUS
STRATEGY CONSULTING | BLOCKCHAIN & SMART CONTRACTS | DATA ANALYTICS

XLAB

TX

KU LEUVEN CiTiP
CENTRE FOR IT & IP LAW

IAIK TU Graz

InfoCert
TINEXTA GROUP

@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