KRAKEN

BROKERAGE AND MARKET PLATFORM
FOR PERSONAL DATA

D7.2 Ethical and legal requirement specification

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

D7.2 Ethical and legal requirement specification

Grant agreement	871473
Work Package Leader	KUL
Author(s)	Jessica Schroers (KUL)
Contributors	Karl Koch (TUG), Wim Vandevelde (KUL), Luca Boldrin (Infocert), Juan Carlos Perez Baun (ATOS), Danaja Fabcic Povse (KUL), Anna Rizzo (Lynkeus), Davide Zaccagnini (Lynkeus)
Reviewer(s)	Alfonso Carcasona Prats (ICERT), Juan Carlos Perez Baun (Atos)
Version	Final
Due Date	30/09/2020
Submission Date	30/09/2020
Dissemination Level	Public

Release History

Version	Date	Description	Released by
v0.1	26/08/2020	Initial version - ToC	Jessica Schroers
v0.2	13/09/2020	Version for Review	Jessica Schroers
v0.3	28/09/2020	Version after review & inclusion new EDPB guidelines 7/2020	Jessica Schroers
v1.0	30/09/2020	Submitted version	Atos

Table of Contents

List of Tables

List of Figures

List of Acronyms

Acronym	Description
CA	Consortium Agreement
CFREU	Charter of Fundamental Rights of the European Union
CJEU	Court of Justice of the European Union
CNIL	Commission nationale de l'informatique et des libertés
DLT	Distributed Ledger Technology
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
ECHR	European Convention of Human Rights
ECtHR	European Court of Human Rights
EDPB	European Data Protection Board
eIDAS	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
ESSIF	European Self-Sovereign Identity Framework
FE	Functional Encryption
GDPR	General Data Protection Regulation
H2020	Horizon 2020
ISP	Internet Service Provider
IP	Internet Protocol
LoA	Level of Assurance
MPC	Multi-Party Computation
QESCD	Qualified Electronic Signature Creation Device
SPoC	Single Point of Contact
SSI	Self-sovereign Identity
TSP	Trust Service Provider
WP	Work Package

Executive Summary

KRAKEN aims to provide a bridge between on the one hand the need for more data for research and innovation and on the other hand the necessity and fundamental right of data subjects to have control over their data. KRAKEN proposes to do this via a marketplace for data, while at the same time providing flexible consent solution, self-sovereign identification and privacy preserving encryption and analysis possibilities. The aim of this deliverable is to provide requirements and guidelines in particular with regard to the GDPR and the eIDAS Regulation, but also to consider ethical aspects and considerations for the KRAKEN solution. After providing a short introduction of KRAKEN and the three technical parts which are developed for the KRAKEN solution, the document gives an overview of legal frameworks which are relevant for KRAKEN, building forth on D2.1 Ethical and legal framework report. This is first the European Convention on Human Rights (ECHR) as well as in the Charter of Fundamental Rights of the European Union (CFREU) in chapter 3, with a special consideration of medical data. In chapter 4 the General Data Protection Regulation (GDPR) is more deeply analysed regarding certain aspects which are in particular relevant for KRAKEN. This part of the deliverable is also the source of most requirements which will be considered in the development of the KRAKEN solution. In chapter 5 the eIDAS Regulation[1] is explained. First a general overview is provided and afterwards the four possibilities of using SSI in KRAKEN are analysed. Chapter 6 gives a short overview on e-Commerce requirements and chapter 7 a general overview of Ethics requirements and considerations on the basis of several fundamental moral principles. Finally, for chapter 8 a first analysis has been made regarding which of the identified requirements can be directly relevant for the three technical parts of KRAKEN which were introduced in the beginning.

This deliverable gives an overview on different requirements and aspects that need to be taken into account during the development of the KRAKEN system, in particular in the work of WP3 (SSI), WP4 (Crypto technologies) and WP5 (Marketplace). The explication of these requirements is only a first step, and the implementation of these requirements has to follow during the project time. The agile approach which KRAKEN uses demands that the requirements will be included in ongoing development work. A first step has been made by the interaction with the Product Owners of the three main scrum teams and a first selection of possibly relevant GDPR requirements for the scrum teams. Many requirements are more organisational than technical and will therefore depend on the organisational approach which KRAKEN would take in a real-life implementation. Nevertheless, requirements and considerations which can be approached during the technical development will be as far as possible implemented in the KRAKEN system by a close collaboration of the different partners of the project.

[1] 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, *OJ* L 257/73, 28.8.2014.

1 Introduction

1.1 Purpose of the document

The purpose of this document is to build on the identified ethical and legal frameworks of T2.1, provide further information and identify ethical and legal requirements. These requirements and guidelines will guide the KRAKEN consortium members in their development of the KRAKEN technologies. This includes a deeper analysis of ethical considerations related to the broader aspects of the KRAKEN technology. This deliverable outlines the relevant ethical and legal requirements and implementation guidelines applicable to the KRAKEN technology.

1.2 Structure of the document

After providing a short introduction of KRAKEN and the three the technical parts which are developed for the KRAKEN solution, the document gives an overview of legal frameworks which are relevant for KRAKEN, building forth on D2.1[2]. This is first the European Convention on Human Rights (ECHR) as well as the Charter of Fundamental Rights of the European Union (CFREU) in chapter 3, including a special consideration of medical data. Afterwards, in chapter 4 the General Data Protection Regulation (GDPR) is more deeply analysed. This is done with special attention to certain aspects which are in particular relevant for KRAKEN and this part of the deliverable is also the source of most requirements which will be considered in the development of the KRAKEN solution. In chapter 5 the eIDAS Regulation is explained, first a general overview is provided and then the four proposed possibilities of using SSI in KRAKEN are analysed. Chapter 6 gives a short overview on e-Commerce requirements and chapter 7 a general overview of Ethics requirements and considerations on the basis of several fundamental moral principles. Finally, chapter 8 includes an analysis which of the identified requirements can be directly relevant for the three technical parts of KRAKEN which were introduced in the beginning.

[2] W. Vandevelde et al., KRAKEN D2.1 Ethical and Legal Framework Report, 31.8.2020, Final.

2 Overview technological aspects KRAKEN

2.1 General overview KRAKEN solution

The main aim of the KRAKEN project is to enhance the data sharing market while respecting the privacy of the data subjects, even when this data shared are personal or special categories of data (often called sensitive data), in a sharply growing data-dependent digital economy.

A large number of personal and sensitive data are collected by different entities from several sources (such as wearables, hospitals, pharmaceutical companies), and domains (health, education, etc.). With the objective to preserve the user data privacy and avoid a misuse of the disclosed data, the KRAKEN project is developing a trusted and secure personal data platform, which supplies tools for citizens (data subjects) to control their own data. The trusted and privacy-preserving approach envisaged by the KRAKEN project provides a secure environment where the sensitive data can be managed using a self-sovereign identity paradigm, so that the data can be shared and traded. The KRAKEN platform will also provide privacy aware advanced data analysis crypto techniques, such as Privacy/Fully Homomorphic Encryption (HE), Functional Encryption (FE) or Multi-Party Computation (MPC), which aim to preserve privacy while keeping the utility of the data. Thus, the KRAKEN platform is based in three main pillars:

- The **Self-Sovereign Identity** (SSI) paradigm, which provides a decentralized user-centric approach on personal data sharing;
- A group of analytic techniques based on cutting-edge **cryptography tools**, which will allow data analysis while preserving data privacy;
- A **data marketplace,** that permits the sharing of personal or sensitive personal data, connecting data buyers and sellers, allowing the data sharing and analytics, which will increase the incomes obtained from the data for both: data buyers and sellers.

2.2 Description Crypto

In order to guarantee the security and privacy of users, one focus of KRAKEN is to research and integrate novel cryptographic means. In particular, the research is focused on

(1) secure end-to-end data-sharing capabilities,

(2) authenticity-preserving and privacy-preserving data analytics, as well as

(3) enhancing the privacy aspects of the KRAKEN SSI system.

Furthermore, the aim is to implement (parts of) the outcome of (1), (2), and (3) in a secure and efficient way.

Specifically, for authenticity-preserving and privacy-preserving data analysis, we will use Multi-Party Computation (MPC) and Functional Encryption (FE). For secure end-to-end data sharing, we investigate post-quantum security and suitable public-key encryption schemes; such as puncturable encryption, which enables fine-grained delegation of decryption rights.

Within the KRAKEN system, these cryptographic means mainly come in to play for the sharing and analysis of (aggregated) personal data of users; such that only the result is revealed to the data consumer, and not more.

2.3 Description planned SSI solution

KRAKEN implements a Self-sovereign identity solution which will support registration and authentication of users toward the marketplace services. The SSI solution can, however, also be used independently, to give access and support the exchange of trusted information with different services – the marketplace being in this perspective one of the possible services.

The SSI solution conforms to the mainstream paradigm which has been proposed in the literature and which is being refined in the relevant communities. It will include an identity wallet (normally, implemented as an app on the user mobile device) and a set of components for the issuing and verification of Verifiable Credentials. It will also include an encrypted backup/restore facility to allow for the recovery of keys and data, which is paramount in the case of a mobile digital identity wallet.

Additionally, the KRAKEN SSI solution will include services and components for the integration with eIDAS services, taking into account the effort of parallel initiatives like the European Self-Sovereign Identity Framework (ESSIF). Specifically:

- it will allow to derive an "identity verifiable credential" from a national identity, leveraging on the eIDAS eID network
- it will allow the creation of an eIDAS signature certificate (advanced or qualified) on the base of an appropriate Verifiable Credential
- it will allow the advanced/qualified signature of a Verifiable Credential and its validation according to eIDAS requirements.

2.4 Description planned Marketplace

KRAKEN will implement a secure, scalable and efficient personal data sharing and analysis platform by adapting state-of-the-art technologies and building on existing computing platforms. The platform will be developed into a data marketplace in two pilot areas: healthcare and education.

Healthcare

The KRAKEN healthcare data marketplace is designed as a GDPR compliant infrastructure for the **sharing of individual biomedical and wellbeing data** by individuals and public/private organizations with interested third parties, in exchange for economic value.

The marketplace will be based on the **integration of established Streamr and MHMD platforms**, and the **technical specifications** defined on the basis of the proposed **user stories**, to be further refined by a collective and bottom-up feedback gathering process (see *T5.1 - User Stories refining*) based on interviews with relevant stakeholders from the research and business domains, as well as a web survey to identify specific needs, key areas of needed functional extension and integration for an optimal definition of user workflows, development specifications, core features and functionalities.

In such a context, the blockchain technology will be enabled by **self-sovereignty identity (SSI) systems for data owners and sellers** for the management of data through the digital wallets. By **keeping record of transactions indefinitely (traceability, immutability)**, the blockchain will guarantee **trust and transparency**, and by allowing to eliminate intermediaries, favoring **collaboration** and **usability of data** for research and business needs. The MHMD blockchain will provide data access control functions while the Streamr blockchain will support payment and purchasing functionalities.

Data trading will involve primarily two kinds of data:

1. health and wellbeing, real-word data *(i.e., heart rate, dietary, physical activity)*, recorded by mobile apps and other wearable devices;

2. **personal health records** *(i.e., lab results, medical histories)* from healthcare facilities

Key stakeholders of the platform, to be authenticated by the KRAKEN wallet-based authentication system (SSI), can be described as follows:

a. data providers: individuals carrying personal data on mobile apps or personal data storage systems; **private and public institutions** *(e.g., hospitals, app and wearable device companies, data brokers, healthcare authorities, data unions)* storing individual data, either consented or where consent can be obtained from individuals using a dynamic consent application;

b. data users: market stakeholders *(e.g., health-tech companies, insurers, public authorities and wellbeing service providers)* interested in acquiring aggregated data sources.

The traded data can be utilized in a variety of fields, including **biomedical research** (e.g., basic and translational research, clinical trials), generation and training of **medical AI algorithms**, **medical device** development and validation, **medical insurance profiling**, as well as the provision of **wellbeing and data analytics services**.

Education

The KRAKEN education marketplace is designed to ease individual and organisations the **sharing and acquisition of education data**, keeping its full control on the owners' hands by different access policies, consents and permissions, whilst including business opportunities for data owners to obtain rewards.

Similarly, its core functionalities and specifications will be based on the definition and refinement of **user stories**, and its architecture will integrate existing data catalogues into a single back-end, including sharing data model capabilities and wallet, payment and transaction functionalities. The credentials and educational data provided will be harmonized and the **Streamr** stack will be adapted and extended to include the integration with University interfaces to get credentials as well as the integration of identity, cryptographic and analytics KRAKEN modules.

The blockchain technology, through the SSI paradigm, will give users control over their data thanks to a digital wallet (including certificates, degrees, learning badges, etc.) enabling to manage it autonomously from the organization which release them, and share it with any other third party total or partially according to their needs. The **security, transparency and immutability** provided by blockchain will guarantee **digital identity and verification of records eliminating the need of intermediaries** and overcoming problems such as falsification, as well as open the door to new and safer ways of **collaboration.**

Data trading will involve the huge amount of data generated by the **education ecosystem**, including certifications, credentials, career paths, courses attended, qualifications, enrolment status.

Key stakeholders of the platform will include:

a. **data providers:** those who yield and/or sell their data to get better services, improve processes or reduce costs. They include **certification providers** *(e.g., universities, training academies, schools, public entities)* and **certification seekers** (*e.g., students, lifelong learners, diploma holders, job seekers*).
b. **data users:** those who buy and/or use data to offer better services or improve their processes. They usually are **certification verifiers** and **certification providers** *(e.g., recruiters, public administration, consultancy companies, education institutions)*.

The use of these data has a huge potential and will provide business value both in educational and job market. Education institutions will be able to provide **better students' experiences** from enrolment to graduation and **advanced services** to manage properly their certifications. On the other hand, recruitment companies and human resources departments will be able to provide **better services** to their job's seekers by facilitating them the verification process and ensuring a fairer system of evaluation of candidates. Governments can also take advantage of education data in order to detect trends and gaps that constitute useful information in **policy-making decision processes**.

3 The right to privacy and the right to data protection

This chapter gives a short overview of the main regulatory instruments regarding the fundamental rights to privacy and data protection and how medical data is considered under the fundamental rights framework. More information regarding these fundamental rights can be found in D2.1[3].

3.1 ECHR and CFREU

The right to privacy

As explained in D2.1[4] is the right to privacy a fundamental human right which can be found in the European Convention on Human Rights (ECHR)[5] as well as in the Charter of Fundamental Rights of the European Union (CFREU)[6], and has been given a broad interpretation by the European Court of Human Rights (ECtHR).

The ECHR is an instrument which defines human rights obligations for the State. These can be 'negative obligations', which means that state actions should not interfere with the rights of individuals, but can also be 'positive obligations' (as interpreted by the ECtHR) which means obligations on the State to secure human rights.[7] The CFREU includes in article 7 the right to privacy, which is the same as in article 8 of the ECHR.[8] As these are State obligations, they do not directly form requirements for the KRAKEN system. Nevertheless, if the right to privacy can be interpreted as an obligation for the State to ensure that privacy guarantees are complied with, it is also in the interest of KRAKEN to ensure that privacy guarantees are applied in the system.[9]

The right to data protection

While not specifically mentioned in the ECHR[10], the right to data protection is a separate right codified in article 8 CFREU. As explained in D2.1[11], in order not to infringe upon article 8 of the CFREU, the personal data must be "*processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law.*" It also states that "*everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.*".[12] These requirements are also included in the General Data Protection Regulation (GDPR), which will be explained in the next chapter.

3.2 Special focus: Medical data

The European Court of Human Rights has judged in several cases that health data/medical data[13] fall under the concept of private life and therefore the protection of art. 8 of the ECHR. The Court ruled that "*The protection of personal data, in particular medical data, is of fundamental importance to a*

[3] W. Vandevelde et al., KRAKEN D2.1 Ethical and Legal Framework Report, 31.8.2020, Final.
[4] W. Vandevelde et al., KRAKEN D2.1 Ethical and Legal Framework Report, 31.8.2020, Final.
[5] Council of Europe, Convention for the Protection of Human Rights and Fundamental Freedoms, 4 November 1950.
[6] Charter of Fundamental Rights of the European Union, OJ C 202/2, 7.6.2016, p. 389-405.
[7] I L Campbell, 'Positive Obligations under the ECHR: Deprivation of Liberty by Private Actors', *Edinburgh Law Review* 10 (2006): 399.
[8] J. Vested-Hansen, 'Respect for Private and Family Life (Private Life, Home and Communications)', in *The EU Charter of Fundamental Rights: A Commentary*, ed. S. Peers et al. (London: Hart Publishing, 2014), 153.
[9] Elisabetta Biasin et al., 'Safecare D3.9 Analysis of Ethics, Privacy, and Confidentiality Constraints', 2018, 14.
[10] But in the court's interpretation since the end of the 1970s/beginning of the 1980s implicitly included in the right to privacy.
[11] W. Vandevelde et al., KRAKEN D2.1 Ethical and Legal Framework Report, 31.8.2020, Final.
[12] Article 8, 2 of the Charter of Fundamental Rights of the European Union.
[13] In the privacy debate the term medical data is more used while in the data protection debate the term health data is preferred, they are here considered to cover the same concept. See E. Biasin, D. Brešić, E. Kamenjašević, P. Notermans, Safecare D3.9 Analysis of ethics, privacy, and confidentiality constraints, 2018, V1, p.15.

person's enjoyment of his or her right to respect for private and family life as guaranteed by Article 8 of the Convention. Respecting the confidentiality of health data is a vital principle in the legal systems of all the Contracting Parties to the Convention. It is crucial not only to respect the sense of privacy of a patient but also to preserve his or her confidence in the medical profession and in the health services in general."[14] As the Court mentioned is respecting the confidentiality of health data also a vital principle in the national legal systems. The legal notion of medical confidentiality is developed in national legal systems.[15] It is usually not absolute, but national law often allows for certain derogations.[16] Also the ECtHR allows for exceptions, as the right to privacy is not an absolute right, but it adopts a strict approach, stating that "any unavoidable interference in this connection should be limited as far as possible to that which is rendered strictly necessary by the specific features of the proceedings and by the facts of the case"[17]. The interest in protecting the confidentiality of medical data might be outweighed by a competing interest, but it is important to consider also the existence of limitations and that abuse is prevented by effective and adequate safeguards.[18]

In general it can be considered that information obtained in a patient-doctor situation covered by medical confidentiality can most likely not be shared via KRAKEN, or only in anonymized form, except if there are national derogations which allow it and the safeguards are provided. This is not a requirement for KRAKEN, but for the data provider if the data provider is for example a hospital. For KRAKEN is relevant that the data provider is legally allowed to share the data, which should be at least confirmed by a declaration of the data provider.

[14] See e.g. Z. v Finland no. 22009/93 (ECtHR, 25 February 1997) para 95; I. v. Finland, no. 20511/03 (ECtHR, 17 July 2008) para 38; K.H. and others v. Slovakia no. 32881/04 (ECtHR, 6 November 2009) para 55.
[15] Biasin et al., 'Safecare D3.9 Analysis of Ethics, Privacy, and Confidentiality Constraints', 17.
[16] Biasin et al., 17–22.
[17] Biasin et al., 21 L.L. v France App No 7508/02 (ECtHR, 10 October 2006) para 45.
[18] Biasin et al., 21.

4 The General Data Protection Regulation

The earlier mentioned article 8 of the ECHR, together with 1981 Council of Europe Convention on Data Protection[19] (Convention 108) formed the inspiration of the 1995 Data Protection Directive[20].[21] The Data Protection was replaced in 2016 by the General Data Protection Regulation (GDPR)[22] , which is applicable since 25 May 2018. This chapter will give an overview on the relevant provisions of the GDPR. The aim of the GDPR is two-fold, to ensure a consistent level of protection for natural persons throughout the European Union while facilitating the free movement of personal data within the internal market.[23] Information on the GDPR and its provisions can be found in D2.1[24], therefore, the focus of this part will be on some particularly relevant areas.

The GDPR does not apply to activities outside scope of Union law, Member States activities in the area of foreign and security policy, processing by competent authorities in the area of criminal offences and public security and in case of personal or household activities of natural persons.[25] If the data provider is a natural person, the question arises whether it might be considered a personal or household activity. However, considering that the information will be made available to a broader group than would be reasonable in case of a household or personal activity, it is unlikely that the household exemption will be applicable. This means that, since KRAKEN will normally entail the processing of personal data, the GDPR will be applicable in that case. In the next sections, specific relevant areas will be explained further, and a general overview of GDPR requirements will be provided.

4.1 Special focus: personal data, special categories of personal data and anonymisation

This sub-section gives an overview of the different types of data, which is relevant to the question whether and how the GDPR is applicable.

4.1.1 Personal data

The GDPR applies to the processing of 'personal data'. The scope of 'personal data' in the GDPR is rather wide and 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"[26]. Included in the definition of personal data is the

[19] Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS No.108, Strasbourg, 28/01/1981, last modernized in 2018 by the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108), Elsinore, Denmark, 18 May 2018.
[20] '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' (n.d.).
[21] Recital 10 and 11 Directive 95/46/EC.
[22] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), *OJ* L 119/1, 4.5.2016.
[23] Recital 13 and 170 GDPR.
[24] W. Vandevelde et al., KRAKEN D2.1 Ethical and Legal Framework Report, 31.8.2020, Final.
[25] Art. 2(2) GDPR.
[26] Art. 4 (1) GDPR.

definition of a data subject, which is an identified or identifiable natural person. This excludes legal persons from the scope of protection of the GDPR.[27]

4.1.2 Special categories of data

In the GDPR are certain categories of personal data considered as special and may only be processed in case of specific circumstances. These data are personal data which reveal or are (art. 9 GDPR):

- racial or ethnic origin,
- political opinions,
- religious or philosophical beliefs,
- trade union membership,
- genetic data,
- biometric data for the purpose of uniquely identifying a natural person,
- data concerning health,
- data concerning a natural person's sex life or sexual orientation.

4.1.3 Anonymous data

Personal data is data that relates to an identified or identifiable natural person. In case data is properly anonymized, the data protection legislation does not apply. However, the threshold for anonymization is rather high.[28]

Academic discussion is still ongoing regarding the scope of anonymization and pseudonymisation. The main issue refers to one of the elements in the definition of personal data: the question whether the data relates to an identified or identifiable person. The Article 29 Working Party considers a natural person as 'identified' when "he or she is "distinguished" from all other members of the group" and 'identifiable' when it is possible to do so.[29] In case the data relates to an identified person it is clear that it is personal data. However, in which case can a person be considered identifiable? A decisive factor in this regard is the concept 'means likely reasonably to be used'. The discussion mainly splits in two approaches, one often called the 'objective' or 'absolute' approach and the other the 'relative' approach regarding the means likely to be used to identify a data subject.[30] The difference is whether the means could be available to anybody (absolute) or only to the controller (relative). Currently the favour seems to be towards the absolute approach, based upon the wording of the GDPR and the Article 29 Working Party opinions.[31]

4.1.3.1 Means likely to be used

The Court of Justice of the European Union (CJEU) decided in the Breyer decision[32] on a question regarding the means likely to be used. However, due to the way the question to the court was phrased, it is not entirely clear whether the court follows the objective or the relative approach.[33] In the Breyer decision, the CJEU considered that the possibility to combine a dynamic IP address with the additional data held by the internet service provider (ISP) could constitute a means likely reasonably to be used

[27] Even though in some Member States such as Austria it is possible that legal persons enjoy data protection under national legislation, see e.g. Decision of the Austrian DPA 2020-0.191.240 of 25.5.2020 (DSB-D124.1182), https://www.ris.bka.gv.at/Dokumente/Dsk/DSBT_20200525_2020_0_191_240_00/DSBT_20200525_2020_0_191_240_00.html, para 49-65.

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

[29] Article 29 Working Party, 'Opinion 4/2007 on the Concept of Personal Data', 20.6.2007, 12.

[30] V I Laan and A Rutjes, 'Privacy-issues bij blockchain: hoe voorkom of minimaliseer je die?', *Computerrecht* 2017, no. 6 (17.10.2017): 10..

[31] Laan and Rutjes.

[32] Patrick Breyer v Bundesrepublik Deutschland, No. ECLI:EU:C:20116:779 / C-258/14 (19.10.2016).

[33] Laan and Rutjes, 'Privacy-issues bij blockchain'..

to identify the data subject. The Advocate General in his opinion, which was followed by the Court, pointed out that it is important to consider whether identification is reasonable. For example, in the case of Germany, legal channels exist to obtain the information from the ISPs and therefore IP addresses are considered personal data. However, it would not be considered personal data if the identification of the data subject was prohibited by law or practically impossible due to the required disproportionate effort in time, cost and man-power, resulting in an insignificant risk of identification.

4.1.4 Pseudonymous data/encrypted data

Often confused with anonymization but different from it is pseudonymisation. As defined in Article 4 (5) pseudonymisation means *"*the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person". Pseudonymised data still falls in the scope of the Regulation and the data protection provisions need to be adhered to (explicitly mentioned in Recital (26): "Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person)".

In the GDPR pseudonymisation is considered as a risk reduction measure which can be used for the implementation of data protection by design and by default. Recital 28 specifically mentions that pseudonymisation can reduce the risks to the data subject and help controllers and processors to meet their data-protection obligations. Pseudonymisation, together with encryption, is considered one of the appropriate safeguards as specified in Article 6 (e) GDPR and is specified as one of the appropriate technical and organizational measures to ensure a level of security appropriate to the risk the processing poses for rights and freedoms of natural persons (Article 32 (1) (a) GDPR). Pseudonymisation (as soon as possible) is considered one of the measures to ensure that the requirements of the Regulation are met, and as a data protection by design and by default measure (see e.g. Recital (78), Article 25 GDPR). This should also be taken into account when developing, designing, selecting or using applications, services and products. For this reason, also producers are encouraged to ensure the ability of controllers and processors to fulfil their data protection obligations. The Regulation therefore actively incentivizes the application of pseudonymisation when processing personal data (see Recital (29)).

Pseudonymised data such as for example encrypted data[34] is in principle still personal data, as it is possible to relate this data to a natural person with additional information, e.g. a key. This would be different for encryption if the key is destroyed and it would therefore not be possible anymore to decrypt the data (assumed that a sufficiently secure encryption algorithm is used), in which case the data could be assumed to be anonymous.[35] This can be relevant especially in relation to DLTs/blockchain. Usually, in case of pseudonymisation or encryption, data protection legislation is still applicable.

4.1.5 KRAKEN

For KRAKEN is important to be able to identify what kind of data will be processed, as the applicability of the GDPR in general and regarding its provisions will depend upon this assessment. Figure 1 gives an overview of questions to be asked to assess what kind of data will be processed.

[34] European Data Protection Board, 'Guidelines 4/2019 on Article 25 Data Protection by Design and by Default', 13.11.2019, 6.

[35] The ICO also suggests data sharding as a replacement for anonymisation/deleting keys (so that data might still be useful): data would be anon to everyone except for the DS, who is the only one who can "re-glue" the shards of data back into PD. https://ico.org.uk/media/for-organisations/documents/1475/deleting_personal_data.pdf.

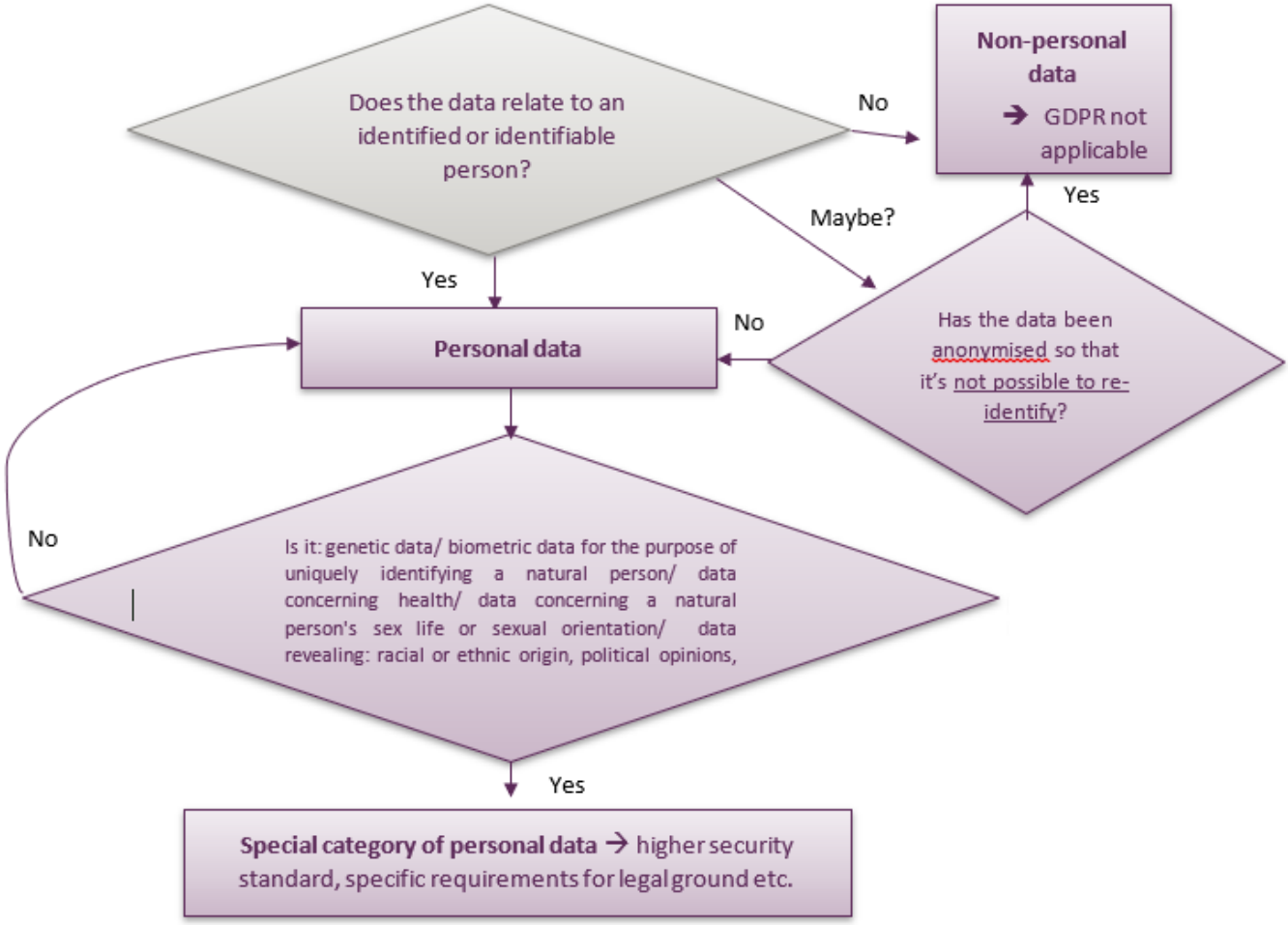


Figure 1: Decision Flowchart Types of Data

Table 1 shows a short overview of different types of data:

Type of data	Description	Applicability GDPR
Non-personal data	Data which is not personal data	GDPR not applicable
Anonymous data	Data which used to be personal data but has been rendered anonymous in such a manner that the data subject is not or no longer identifiable	GDPR not applicable
Personal data	Data which relates to an identified or identifiable person	GDPR is applicable
■ Pseudonymous data	Personal data which has been processed in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept	GDPR is applicable

	separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person (art. 4 (5) GDPR)	
■ Special category of data	personal data which reveal or are: • racial or ethnic origin, • political opinions, • religious or philosophical beliefs, • trade union membership, • genetic data, • biometric data for the purpose of uniquely identifying a natural person, • data concerning health, • data concerning a natural person's sex life or sexual orientation. (art. 9 GDPR)	GDPR is applicable, special requirements

Table 1 Overview different types of data

4.2 Special focus: Controller – Processor

The GDPR, and the Data Protection Directive before it, use different roles in order to appoint certain responsibilities to actors. The natural person whose data is processed is the data subject, and the other two important roles are the role of the data controller and the role of data processor.

4.2.1 Controller

Establishing who is controller is important since the controller is the one responsible for the personal data, and to whom therefore most of the legal requirements apply. The data controller is the "natural or legal person, public authority, agency or any other body which, alone or jointly with others, determines the purposes and means of the processing of personal data" (art. 4 (1) GDPR). Different from the Directive, the GDPR added to this definition that the controller or the specific criteria for its nomination may be provided by law in case the purposes and means are determined by Union or Member State law (art. 4 (7) GDPR). In general, however, the allocation of the notion of controller is based on its concrete activities in a specific context. It should be noted that the assessment of the status is based upon a factual assessment, depending on who determines the purposes and means, while contractual arrangements can only provide an indication and always need to be checked against the factual circumstances.[36]

[36] European Data Protection Board, 'Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR', 2.9.2020, 9.

4.2.2 Joint controllers

It is also possible that several controllers are involved in a data processing. In case they jointly determine the purposes and means of processing, they are considered joint controllers (art. 26 (1) GDPR). In case of joint control, the controllers are obliged to make an arrangement between them, specifying their respective roles and responsibilities, in particular toward the data subject as they have to ensure the exercise of the data subject rights and information duties (art. 26 GDPR).

The European Court of Justice (CJEU) judged on joint controllership in three recent decisions: *Wirtschaftsakademie*[37], *Jehovan todistajat*[38] and *Fashion ID*[39]. In these cases respectively the questions were decided whether an administrator of a fan page on Facebook, a religious community, or a website administrator who embedded a Facebook Like button on his website, can be considered a joint controller.[40] Even though it was decided under the Data protection Directive, the decisions are still relevant for the GDPR.

In all cases, the CJEU consistently reiterates the aim of the Data protection Directive to ensure a high level of protection of the fundamental rights and freedoms of natural persons[41], the fact that access to the personal data by every controller is irrelevant in case of joint controllership,[42] and that joint control does not mean equal responsibility[43]. In both 'Facebook cases' the Court considered the responsibility of the non-Facebook controller greater in case the natural persons whose personal data are processed do not have a Facebook account. [44]

In the recent EDPB guidelines further information on the definition of joint controllers is provided. As explained by the EDPB, joint participation can be in different forms, it can be for example in the form of a common decision or can result from converging decisions of the controllers regarding the purposes and essential means.[45] A common decision is the traditional understanding of joint control whereby the controllers decide together, while the case of converging decisions arises from the earlier mentioned case law of the CJEU. If controllers do not take joint decisions, but the decisions they take are converging on purposes and means since they complement each other and "are necessary for the processing to take place in such manner that they have a tangible impact on the determination of the purposes and means of the processing"[46] they are considered to be converging decisions.[47] In these cases the controllers are joint controllers, in respect of those operations for which they determine jointly the means and purposes of the processing.

4.2.3 Processor

Finally, the processor is the "natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller" (art. 4 (8) GDPR). The processor is always acting

[37] CJEU 5 June 2018, C-210/16, ECLI:EU:C:2018:388 ('*Wirtschaftsakademie* case').
[38] CJEU 10 July 2018, C-25/17, ECLI:EU:C:2018:551 ('*Jehovan todistajat* case').
[39] CJEU 29 July 2019, C-40/17, ECLI:EU:C:2019:629 ('*Fashion ID* case').
[40] For more information see C. Ducuing and J. Schroers, 'The recent case law of the CJEU on (joint) controllership: have we lost the purpose of 'purpose'?', Computerrecht (forthcoming).
[41] First referred to in CJEU 13 May 2014, C-131/12, ECLI:EU:C:2014:317 (Google Spain), para 34; *Wirtschaftsakademie* case, n 19, para 28; *Jehovan todistajat* case, n 20, para 35; *Fashion ID* case, n 21, para 65-66.
[42] *Wirtschaftsakademie* case, n 19, para 38; *Jehovan todistajat* case, n 20, para 69; *Fashion ID* case, n 21, para 69 and 83.
[43] *Wirtschaftsakademie* case, n 19, para 43; *Jehovan todistajat* case, n 20, para 66; *Fashion ID* case, n 21, para 70 and 85.
[44] *Wirtschaftsakademie* case, n 19, para 41; *Fashion ID* case, 21, para 83.
[45] European Data Protection Board, 'Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR', 18.
[46] European Data Protection Board, 18.
[47] European Data Protection Board, 18.

under the authority of the controller, as soon as the processor processes the data for their own purposes and determine their own means, it would be considered a controller.

Accordingly, the same entity may act at the same time as a controller for certain processing operations and as a processor for others and the qualification as controller or processor should be assessed with regard to specific sets of data or operations.[48]

4.2.4 KRAKEN

Table 2 Overview possible controller-processor situations KRAKEN gives and overview which different situations can in principle occur:

Data provider	What Data will be provided?	GDPR actor	KRAKEN acting	GDPR actor	What data will be provided?	Data buyer – GDPR actor	Nr. Of contr ollers
Origin controller	Anonymous data	*GDPR not applicable*	N/A	N/A	N/A	N/A	0 [1]
	Personal data	**Controller**	Only upon instructions of the Origin controller or Receiving controller	Processor	Personal data	**Controller**	2
					Anonymous data	*GDPR not applicable*	1
			Determining own means and purposes	**Controller**	Personal data	**Controller**	**3**
					Anonymous data	*GDPR not applicable [except possible Joint Control]*	*2*
Data subject	Personal data	Data subject	Only upon instructions of the Receiving controller	Processor	Personal data	**Controller**	1
			Determining own means and purposes	**Controller**	Personal data	**Controller**	**2**
					Anonymous data	*GDPR not applicable [except possible Joint Control]*	*1*

Table 2 Overview possible controller-processor situations KRAKEN

It is important to identify whether KRAKEN is a controller or processor, as this is relevant for the applicable requirements. Accordingly, the overview of GDPR requirements in section 4.7 is divided up in requirements for controllers, processors or both.

[48] European Data Protection Board, 11.

For account data it can be assumed that KRAKEN will generally be the controller. With regard to content data the assessment is more difficult. In principle, the intention is that KRAKEN will only provide a platform to exchange data and will for that provide a catalogue with information about the data but will normally not store the data itself. It is possible that KRAKEN would transfer the data, if a data provider and data buyer have agreed to transfer data. In that case KRAKEN could provide a safe way for transfer. Furthermore, KRAKEN can provide the possibility to analyse data. The intention is that all these actions would only be done upon instructions of the data buyer (the receiving controller), and that KRAKEN would only act as processor. However, considering that the assessment of controller and processor is a factual one, KRAKEN needs to be careful not to overstep the boundaries and become unintentionally a controller with regard to content data. It is therefore important that KRAKEN has a controller-processor agreement with the receiving controllers and will always act only upon instructions of the receiving controllers.

4.2.5 Controller-processor agreement

The controller is obliged to conclude a contract with the processor which must include at least[49]:

- The processor processes the personal data only on documented instructions from the controller;
- The processor only transfers personal data to a third country or an international organization on documented instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;
- Persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
- The processor takes the required security measures;
- The processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes;
- Where a processor engages another processor, the same data protection obligations as set out in the contract between the controller and the processor shall be imposed on that other processor by way of a contract, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Regulation;
- Taking into account the nature of the processing, the processor shall assist the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights;
- The processor assists the controller in ensuring compliance with the obligations regarding security, notification of data breach and Data Protection Impact Assessments (DPIAs), taking into account the nature of processing and the information available to the processor;
- At the choice of the controller, the processor deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data;
- The processor makes available to the controller all information necessary to demonstrate compliance with these obligations and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller;

[49] Art. 28 GDPR.

- The processor immediately informs the controller if, in its opinion, an instruction infringes this Regulation or other Union or Member State data protection provisions.

4.3 Special focus: Consent

This section gives an overview on the requirements for valid consent and the different types of consent, since the exchange of content data will most likely be based on the legal basis of consent.

4.3.1 Requirements for valid consent as a legal basis for processing

Consent is one of the six legal grounds which can make processing lawful.[50] Consent is considered to be "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her".[51] Based on art. 4 and art. 7 GDPR, the following requirements can be identified, as shown in table 3:

Indication of the data subject's wishes which signifies agreement to the processing of his/her personal data	Explanation
Freely given	This means that the data subject has a real choice and control.[52] This means that for example if the consent is non-negotiable tied to the terms & conditions, it is not considered to be freely given.[53] If the consent is not necessary to the performance of a contract, but the consent is presented as conditional for it, it is also not freely given.[54] If the data subject is not able to refuse or withdraw consent without detriment, it is not considered to be freely given. [55] If there is an imbalance of power which gives the data subject the impression that it cannot refuse the consent, then the consent is not freely given. ➔ **The consent is invalid if the data subject is not able to exercise their free will.**[56]
Specific	The consent should be given in relation to one or more specific purposes. This should provide the data subject with a degree of control and transparency.[57] The controller must apply[58]: - Purpose specification - Granularity in consent requests

[50] Art. 6(1)(a) GDPR.
[51] Art. 4 (1) (11) GDPR.
[52] European Data Protection Board, 'Guidelines 05/2020 on Consent under Regulation 2016/679', 4 May 2020, 7.
[53] European Data Protection Board, 7.
[54] Art. 7 (4) GDPR.
[55] European Data Protection Board, 'Guidelines 05/2020 on Consent under Regulation 2016/679', 7.
[56] European Data Protection Board, 8.
[57] European Data Protection Board, 14.
[58] European Data Protection Board, 14.

	- Clearly separate the information for obtaining consent from other information ➔ **The data subject should be able to understand for which specific purpose s/he gives consent to the processing**. ! if afterwards the purpose is changed, a new consent needs to be requested & if consent for different purposes is requested, it needs to be asked individually for each purpose. + for each separate consent request information should be added about the data that are processed for each purpose.[59] Exception for scientific research: according to recital 33 GDPR there is an exception for scientific research, as it is often not possible to fully identify the purpose of personal data processing at the time of collection. Here it is possible to give consent to certain areas of scientific research. Recognised ethical standards for scientific research must be complied with, and data subjects should have the possibility to give only consent to certain areas of research. For more information, see section 4.4.
Informed	The data subject must be provided with accessible information (transparency requirement) before giving their consent, so that they can make informed decisions. The following information must at least be provided[60]: - Controller's identity; - Purpose of each of the processing operations; - What (type of) data will be collected and used; - Information on the right to withdraw consent; - If relevant: information on the use of the data for automated decision making; - If relevant: the possible risks of data transfers and appropriate safeguards, if no adequacy decision is in place. For more information see section 4.3.4.
Unambiguous	The consent should be an unambiguous indication of the wishes of the data subject. This requires a statement or clear affirmative act, which excludes silence or inactivity of the data subject and therefore also pre-ticked boxes.
Controller must demonstrate that the data subject has consented to the processing	The burden of proof is on the data controller, who can decide how to comply with this provision, but it should not result in excessive amounts of additional data processing.[61] The controller can keep records of the consent to show how and when the consent was obtained and which information was given to the data subject.[62] A recommendation is to refresh the consent from time to time in order to ensure that the data subject stays well informed.[63]

[59] European Data Protection Board, 15.
[60] European Data Protection Board, 15.
[61] European Data Protection Board, 22.
[62] European Data Protection Board, 23.
[63] European Data Protection Board, 23.

Possibility to withdraw consent at any time, must be as easy to withdraw as to give consent	Withdrawing the consent should be as easy as giving it, which does not mean that it must be via the same action, but only that it must be as easy as the consent-giving action.[64] If consent can be given by one mouse-click, data subjects should be able to withdraw consent equally easily.[65] If consent is given in a specific user interface (e.g. a website, app, IoT device interface), the withdrawal should be possible in the same user interface, as changing to another user-interface would require additional effort.[66] The withdrawal should be free of charge and without unduly lowering service levels.[67]
Before giving consent, the data subject must be informed that a withdrawal shall not affect the lawfulness of processing based on consent before its withdrawal	This is part of the requirement that the data subject must be informed. If consent is withdrawn, the processing operations based on consent which happened before the withdrawal of consent stay lawful, but any processing operations must be stopped from the moment the consent has been withdrawn. [68] In case the data are only processed on the basis of consent, then they should be deleted when the consent has been withdrawn. [69]

Table 3 Consent information

4.3.2 Consent for the processing of special categories of personal data

The processing of special categories of personal data (e.g. health data) is normally prohibited. However, art. 9 (2) GDPR provides several exemptions of this prohibition. One of them is that the data subject has given explicit consent to the processing of those personal data for one or more specified purposes. Nevertheless, when Union or Member State law provide that the prohibition may not be lifted by the data subject, then this exception is not applicable. For more information on Member State provisions see section 4.6.

Explicit consent: Normal consent is not sufficient in case of higher risks, such as the processing of special categories of personal data, data transfers to third countries without an adequacy decision, or automated decision making. [70] In such cases is explicit consent required.[71] It means that, more than just an unambiguous statement, the data subject has to give an express statement of consent. There is no explicit information on how that should be done, nevertheless, the European Data Protection Board (EDPB) gives some examples how it could be done: the most obvious way is to give consent in a written statement, best signed by the data subject.[72] Other possibilities to give an express statement could be to fill in an electronic form, send an email or upload a document with the signature of the

[64] European Data Protection Board, 23.
[65] European Data Protection Board, 23.
[66] European Data Protection Board, 23.
[67] European Data Protection Board, 23.
[68] European Data Protection Board, 24.
[69] European Data Protection Board, 24.
[70] European Data Protection Board, 20.
[71] European Data Protection Board, 20.
[72] European Data Protection Board, 21.

data subject. [73] In order to make sure that the consent is indeed intended by the data subject, two stage verification of the consent can be useful.[74]

4.3.3 Consent for scientific research (non-GDPR)

With regard to scientific research, certain distinctions need to be made. There is data protection consent (section 4.3), with the acceptance of a broader purpose for scientific research purposes (see section 4.4.2). Next to this, legislation or other provisions might additionally require the consent of the human participants to research, as is the case with regard to the informed consent required in the H2020 research ethics framework (see D7.1[75]) or the Clinical Trials Regulation. The EDPD considers this type of consent not necessarily as a legal basis for processing.[76] The informed consent requirement for the protection of individuals in trials or experiments is an independent provision which is substantially different from safeguarding only the protection of their personal data.

4.3.4 Inform the data subject

The data subject must be informed about the processing of their personal data, which is a general obligation but especially important in case of consent, to make sure that the consent is indeed an informed consent. The controller therefore has to inform the data subject with regard to[77]:

- the identity and the contact details of the controller and, where applicable, of the controller's representative;
- the contact details of the data protection officer, where applicable;
- the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
- where the processing is based on legitimate interest of the controller, the legitimate interests pursued by the controller or by a third party;
- the recipients or categories of recipients of the personal data, if any;
- where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers of personal data to third countries or international organisations which are not based on an adequacy decision, reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.
- the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
- the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;
- where the processing is based on consent, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
- the right to lodge a complaint with a supervisory authority;

[73] European Data Protection Board, 21.
[74] The EDPB gives the example that the data subject receives an e-mail with the necessary information and the request to consent to the processing by replying “I agree”, after which the agreement is confirmed by clicking a verification link or an SMS with a verification code.
[75] Danaja Fabcic et al., KRAKEN D7.2 Ethical and legal management report, 31.7.2020, Final.
[76] European Data Protection Board, ‘Guidelines 05/2020 on Consent under Regulation 2016/679’, 30.
[77] Art. 13 and 14 GDPR.

- the existence of automated decision-making, including profiling, and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.
- In case of further processing for another purpose: information on the other purpose
- If the personal data is obtained directly from the data subject: whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;
- If the personal data is not directly from the data subject: from which source the personal data originate, and if applicable, whether it came from publicly accessible sources.

Exceptions exist for indirectly obtained personal data, it is not necessary to inform the data subject, if:

- the data subject already has the information;
- the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to conditions and safeguards or if the obligation to inform is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available;
- obtaining or disclosure is expressly laid down by Union or Member State law to which the controller is subject and which provides appropriate measures to protect the data subject's legitimate interests; or
- the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy.

4.4 Special focus: research exemption

Scientific research, together with archiving purposes in the public interest, historical research and statistical purposes, has a special status in the GDPR and can enjoy certain exemptions. So is for example further processing for these purposes not considered to be incompatible with the initial purposes[78], data may be stored for longer periods if it is solely for these purposes[79] and special categories of data may be processed for these purposes[80]. This does not mean a carte blanche permission, since at the same time the fundamental rights and interests of the data subject should always be safeguarded, by technical and organizational measures or based upon Union or Member State law which provides safeguards. The main article relating to these purposes is art. 89 GDPR, which provides safeguards and derogations relating to the processing for the mentioned purposes. Regarding the safeguards, the GDPR provides that they should be appropriate to safeguard the rights and freedoms of the data subject and ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimization.[81] If the purpose can be fulfilled with pseudonymisation or anonymization of the data, then this should be applied.[82] Member States may also provide for derogations of the certain data subjects rights for these purposes, for more information on national provisions see section 4.6.

[78] Art. 5 (1) (b) GDPR.
[79] Art. 5 (1) (e) GDPR.
[80] Art. 9 (2) (j) GDPR, based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.
[81] Art. 89 (1) GDPR.
[82] Art. 89 (1) GDPR.

4.4.1 What is scientific research?

The GDPR does not provide a definition of the term 'scientific research'.[83] Even though recital 159 indicates that scientific research purposes should be interpreted in a broad manner, the EDPB states that it should be understood in the common meaning of scientific research and mean "a research project set up in accordance with relevant sector related methodological and ethical standards, in conformity with good practice" [84].

4.4.2 Consent for scientific research (GDPR)

Recital 33 includes some flexibility with regard to the degree of specification of purpose in case of scientific research, as it is often not possible to specify the exact purposes at the time of collection. Nevertheless, this does not mean that no purpose needs to be provided, instead, recital 33 allows a more general description of purpose.[85] The processing of special categories of personal data will, even considering recital 33, be "subject to a stricter interpretation and requires a high degree of scrutiny"[86]. When it is not possible to fully specify research purposes, then the EDPB requires that other ways should be sought in order to preserve the essence of the consent requirements. Possible ways to ensure that are for example that the data subject could consent to a general research purpose and specific stages of a research project, and consent for subsequent steps can be obtained when the next stage begins. Another possibility is to add additional safeguards such as data minimization, anonymization and data security; and to ensure transparency, so that the data subject has "at least a basic understanding of the state of play, allowing him/her to assess whether or not to use, for example, the right to withdraw consent"[87]. This includes for example having a comprehensive research plan available which specifies the research questions and working methods as clearly as possible, and having a specific contact point in case of questions.[88] Even though withdrawal of consent could undermine the scientific research, the GDPR does not include an exemption for this for scientific research. Therefore, if the data subject wishes to withdraw consent for processing for scientific purposes, the controller must stop processing the data and delete it if possible.[89]

4.5 Special focus: DPIA

Recital 89 of the GDPR explains that the general obligation to notify personal data processing to supervisory authorities did not substantially improve the protection of personal data and has therefore been abolished in the GDPR. Instead the aim of the GDPR is to establish effective procedures and mechanisms for processing operations which could form a high risk to the rights and freedoms of natural persons. The measure of choice in those cases is a data protection impact assessment (DPIA) which should be carried out by the controller before the processing takes place. This is done in order to assess the particular likelihood and severity of high risks, taking into account the nature, scope, context and purposes of the processing and the sources of the risk. The measures, safeguards and mechanisms to mitigate the risk should be included in the data protection impact assessment.

[83] European Data Protection Board, 'Guidelines 05/2020 on Consent under Regulation 2016/679', 30.
[84] European Data Protection Board, 30.
[85] European Data Protection Board, 30.
[86] European Data Protection Board, 30.
[87] European Data Protection Board, 31.
[88] European Data Protection Board, 31.
[89] European Data Protection Board, 32.

4.5.1 When is a DPIA required?

A DPIA does not need to be conducted for every processing but is required for those which may result in risks for the rights and freedoms of natural persons.[90]

Likely to result in a risk?

Risk is mostly assessed in terms of likelihood and severity/seriousness. Most risk management procedures address risks for organizations and their activities.[91] A risk assessment in the field of data protection is different, as the GDPR defines that the risk which needs to be assessed is the risk to the rights and freedoms of natural persons.[92]

The assessment in numerical values given for the likelihood and severity is criticized, as for example the severity of an impact on data subjects cannot be measured in numbers.[93] Currently no generally agreed way to assess risk in the field of privacy and data protection exists, even though several guidance documents are available.

The GDPR does not define a specific model, but states that in order to assess whether processing operations involve a risk or a high risk, an objective assessment should be made of the severity and likelihood of the risk to the rights and freedoms of the data subject, which is determined by looking at the nature, scope, context and purposes of the processing.[94]

Therefore, currently only indications exist on how to assess the risk:

[90] Art. 29 Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, WP 248 rev. 01, adopted on 4 April 2017, as last revised and adopted on 4 October 2017, p.8.

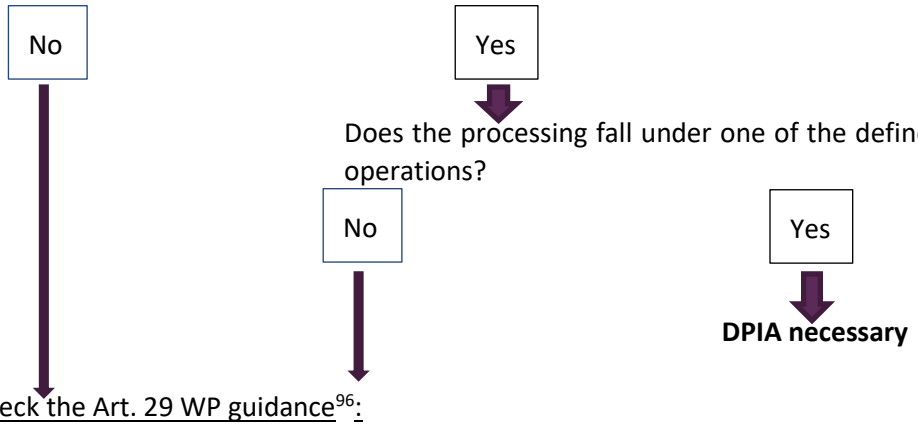
[91] Felix Bieker et al., 'A Process for Data Protection Impact Assessment Under the European General Data Protection Regulation', in *Privacy Technologies and Policy*, vol. 9857, Lecture Notes in Computer Science (Cham: Springer International Publishing, 2016), 24, http://link.springer.com/10.1007/978-3-319-44760-5.

[92] art. 35 (1) GDPR, recital 77 GDPR.

[93] Felix Bieker, Marit Hansen, and Michael Friedewald, 'Die Grundrechtskonforme Ausgestaltung Der Datenschutz-Folgeabschätzung Nach Der Neuen Europäischen Datenschutz-Grundverordnung', Zeitschrift für Datenschutz-, Informations- und Kommunikationsrecht, no. 4 (2016): 193.

[94] Recital 76 GDPR.

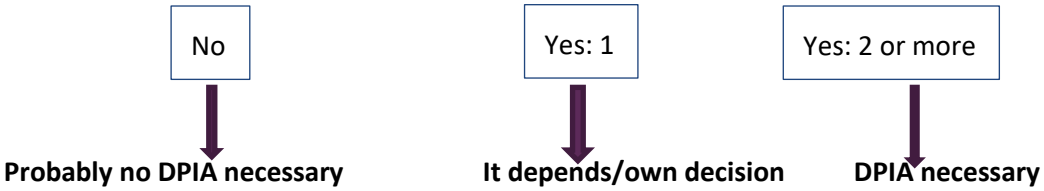
1) Did the national supervisory authority establish a list of processing operations which require a DPIA[95]?



1) Check the Art. 29 WP guidance[96]:

Does the processing involve one of the following?

- ☐ Evaluation or scoring, including profiling and predicting, especially from "aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements" (recitals 71 and 91)
- ☐ Automated-decision making with legal or similar significant effect
- ☐ Systematic monitoring
- ☐ Sensitive data or data of a highly personal nature
- ☐ Data processed on a large scale: considering e.g.
  - the number of data subjects concerned, either as a specific number or as a proportion of the relevant population;
  - the volume of data and/or the range of different data items being processed;
  - the duration, or permanence, of the data processing activity;
  - the geographical extent of the processing activity
- ☐ Matching or combining datasets, for example originating from two or more data processing operations performed for different purposes and/or by different data controllers in a way that would exceed the reasonable expectations of the data subject
- ☐ Data concerning vulnerable data subjects (recital 75)
- ☐ Innovative use or applying new technological or organisational solutions
- ☐ When the processing in itself "prevents data subjects from exercising a right or using a service or a contract" (Article 22 and recital 91)



For KRAKEN no risk is expected during the project time, however, considering that a real life KRAKEN system would aim for processing data on a large scale and that KRAKEN could on the one hand possibly match and combine data sets using new technological or organizational solutions, and possibly even

[95] E.g. Germany: https://www.datenschutzkonferenz-online.de/media/ah/20181017_ah_DSK_DSFA_Muss-Liste_Version_1.1_Deutsch.pdf; France: https://www.cnil.fr/fr/liste-traitements-aipd-requise; UK: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/examples-of-processing-likely-to-result-in-high-risk/.

[96] 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', 4 October 2017.

sensitive data, it is to be expected that a DPIA is needed for the final implementation. D8.3 will include an evaluation whether a DPIA should be conducted. During the research and development of KRAKEN a preliminary (research) DPIA is planned in order to identify first risks, even though, as there is no definitive implementation of the system yet, it is not possible to conduct a complete DPIA.

4.5.2 DPIA

At the moment no European wide standard DPIA exists. The GDPR does not refer to a specific model for a DPIA, but states the minimum requirements for carrying out a DPIA.[97] A data protection impact assessment contains at least:

1) a systematic description of the envisaged processing operations and the purposes of the processing, and in case the legitimate interest of the controller is considered the legal ground for processing, it also includes the legitimate interest;

2) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;

3) an assessment of the risks to the rights and freedoms of data subjects; and

4) the measures envisaged to address the risks (e.g. safeguards and security measures).

Different national Data Protection Authorities (DPAs) have defined approaches and guidance for DPIAs. When analysing the KRAKEN system, in particular the one of the French Commission nationale de l'informatique et des libertés (CNIL)[98] and the German Standard Data Protection Model[99] will be taken into account. The results will be included in D7.3.

4.5.3 After a DPIA

A DPIA can have several outcomes:

In case the DPIA indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk, the competent data protection authority needs to be consulted (art. 36 GDPR). Certain information needs to be provided to the supervisory authority, including the DPIA. The supervisory authority shall then provide written advice within a period of maximum eight weeks (which may be extended by six weeks if the intended processing is very complex), and the periods may be suspended until the supervisory authority has obtained all requested information.[100] In case a supervisory authority does not consider it possible to bring processing operations into compliance with the Regulation, it has the power to impose a ban on processing.[101]

In case the DPIA indicates that the processing would not result in a high risk, and that the measures taken mitigate the risk, there are no specific rules. Considering the general documentation requirement (art. 30 GDPR, recital (82)), it is advisable that the controller keeps the records of the DPIA in order to demonstrate compliance with the Regulation and the supervisory authority can request the information.[102] For transparency reasons it would be useful to publish at least a shortened version of

[97] art. 35 (7) GDPR.
[98] See https://www.cnil.fr/en/privacy-impact-assessment-pia.
[99] Conference of the Independent Data Protection Supervisory Authorities of the Federation and the Länder, 'The Standard Data Protection Model - A Method for Data Protection Advising and Controlling on the Basis of Uniform Protection Goals', 17.4.2020.
[100] art. 36 (2) GDPR.
[101] art. 58 (2) (f) GDPR.
[102] art. 58 (1) (a) GDPR

the DPIA report.[103] For example, the Belgian DPA states that a rapport which needs to be dated and in writing must exist and an intern mandated body within the company which is responsible for decisions must regularly be informed of the status of the risk analysis and is required to formally approve the assessment and the measures taken.[104]

In case the risk changes at any point after the DPIA, a new iteration of the DPIA might be required.[105]

4.6 Special focus: national implementation and restrictions on sharing personal data

This section outlines the most important rules from national GDPR implementations for a selected number of EU countries.[106]

4.6.1 Belgium[107]

Age of consent for ISS[108]

A child must be a minimum of 13 years old to give their consent to processing in relation to ISS.

Sensitive personal data

In case of processing of genetic, biometric, or health data, the controller (or, where applicable, the processor) must:

1) maintain a list of the categories of persons having access to the personal data, including a description of their role in connection with the processing of the data, which must be disclosed to the competent DPA on request, and;
2) make sure that the people designated are bound by a legal, statutory or contractual obligation of confidentiality with regard to the processed personal data.

Controller and processor – DPIA and DPO

A DPO is required in case of processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, if the processing is likely to result in a high risk of violating the rights and freedoms of data subjects. The DPO is subject to secrecy obligations under national law.

Processing for scientific research purposes

---

[103] Felix Bieker, Marit Hansen, and Michael Friedewald, 'Die Grundrechtskonforme Ausgestaltung Der Datenschutz-Folgeabschätzung Nach Der Neuen Europäischen Datenschutz-Grundverordnung', 196.

[104] Commissie voor de bescherming van de persoonlijke levenssfeer, Aanbeveling nr. 01/2018 van 28 februari 2018, Bijlage 1.

[105] art. 35 (11) GDPR.

[106] The information provided in this section was obtained from https://www.whitecase.com/publications/article/gdpr-guide-national-implementation (last consulted on 23 September 2020).

[107] The national GDPR implementation of Belgium can be consulted on: https://www.ejustice.just.fgov.be/mopdf/2018/09/05_1.pdf#Page10 (last consulted on 23 September 2020).

[108] 'ISS' is the abbreviation for 'Information Society Service', defined as: "*any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services*" under Article 1, 1, (b) of Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (codification).

Derogations from the right of access (art. 15), the right to rectification (art. 16), the right to restriction of processing (art. 18), and the right to object (art. 21).

Controllers may apply derogations to these data subject rights in case the exercise of these rights are likely to render impossible or seriously impair the achievement of the research purposes, and such derogations are necessary. The controller must use anonymized data, pseudonymized data, or non-pseudonymized data depending on whether or not the research purposes can be achieved with these types of data. Re-identification of personal data is only allowed in case it is necessary for the research purposes.

4.6.2 Denmark[109]

Personal data of deceased persons

The Data Protection Act and GDPR apply to personal data for ten years after death.

Legal bases for processing

When personal data (including sensitive personal data) have been processed for the purpose of carrying out statistical or scientific studies of significant importance to society, then the personal data may not subsequently be processed for other than scientific or statistical purposes, even with the consent of the data subject.

Age of consent for ISS

A child must be a minimum of 13 years old to give their consent to processing in relation to ISS.

Sensitive personal data

The Act on Research Ethics Review of Health Research Projects contains conditions and limitations for the processing of genetic, biometric and health data in health research projects.[110]

Exemptions to data subject rights

The right to be provided information (art. 14) does not apply if:

1) the data subject's interest in the information is found to be overridden by essential considerations of private interests, including considerations relating to the data subject; or
2) the data subject's interest in obtaining this information is found to be overridden by essential considerations of public interests found in Article 23 of the GDPR (*e.g.* national security, national defence, public security, etc.).

Restrictions to data subject rights

The right to information (art. 13), the right of access (art. 15) and the communication of a personal data breach (art. 34) do not apply if:

1) the data subject's interest in the information is found to be overridden by decisive considerations of private interests, including considerations relating to the data subject; or
2) the data subject's interest in obtaining this information is found to be overridden by essential considerations of public interests found in Article 23 of the GDPR (*e.g.* national security, national defence, public security, etc.).

[109] The national GDPR implementation of Denmark can be consulted on: https://www.datatilsynet.dk/media/7753/danish-data-protection-act.pdf (last consulted on 23 September 2020).

[110] The Act on Research Ethics Review of Health Research Projects can be consulted on: https://en.nvk.dk/rules-and-guidelines/act-on-research-ethics-review-of-health-research-projects (last consulted on 23 September 2020).

The right of access (art. 15), the right to rectification (art. 16), the right to restriction (art. 18) and the right to object (art. 21) do not apply if the personal data is only processed for scientific or statistical purposes.

International data transfers

The DPA may, in absence of an adequacy decision and if the case is exceptional, prohibit, restrict or suspend the transfer of sensitive personal data to a third country or international organization.

Processing for scientific research purposes

Sensitive personal data processed for the purpose of statistical or scientific studies with significant importance to society may generally be disclosed to a third party processing the data for the same purposes. However, such data may only be disclosed to a third party with prior authorization from the DPA, in case such disclosure:

1) is made for the purpose of processing outside the territorial scope of the GDPR;
2) relates to biological material, or;
3) is made for the purpose of publication in a recognized scientific journal or similar publication.

4.6.3 Estonia[111]

Personal data of deceased persons

Consent of a data subject is valid for ten years after death (20 years for minors).

Age of consent for ISS

A child must be a minimum of 13 years old to give their consent to processing in relation to ISS.

Sensitive personal data

The Human Genes Research Act sets out rules for the processing of genetic data for the purposes of genetic research and personalized medicine.

Exemptions to data subject rights

Specific exemptions to the right to erasure (art. 17) in sectoral legislation (*e.g.* fraud prevention, risk management, security reasons, etc.) and in case of archiving in the public interest insofar the exercise of this right is likely to impede that public interest.

Exceptions to not be subject to a decision solely based on automated processing (art. 22) in specific situations, for example where personal data are processed for the purposes of archiving in the public interest, scientific or historical research purposes, or statistical purposes, and the exercise of this right is likely to significantly impede those purposes.

Restrictions to data subject rights

Specific restrictions, for example where personal data are processed for the purposes of archiving in the public interest, scientific or historical research purposes, or statistical purposes, insofar as the exercise of these rights is likely to make the achievement of the objectives of those purposes impossible or impedes it to a significant extent.

Controller and processor – DPIA and DPO

The data subject may require full or partial compensation from all joint controllers, from any of them or from some of them separately. If one of them has performed the obligation in full, the other solidary obligors are not liable to the data subject. Between themselves, the joint controllers are liable for the

[111] The national GDPR implementation of Estonia can be consulted on: https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/523012019001/consolide (last consulted on 23 September 2020).

performance of the obligation in equal shares unless otherwise provided by the law (the GDPR) or a contract (*e.g.* limitation of liability).

Processing for scientific research purposes

If sensitive personal data are processed for scientific or historical research purposes, the relevant ethics committee (or DPA in absence of an ethics committee) must first verify compliance with the applicable rules.

4.6.4 Finland[112]

Age of consent for ISS

A child must be a minimum of 13 years old to give their consent to processing in relation to ISS.

Sensitive personal data

Additional requirements under the Act on the Secondary Use of Health and Social Data for the secondary use of health data for registered based health research.

Exemptions to data subject rights

Exemptions to the right to information (art. 14) possible if:

1) it is necessary for the protection of national security, defence or public order or security;
2) it is necessary for the prevention or investigation of crime;
3) it is necessary for carrying out the monitoring function pertaining to taxation or the public finances; or
4) providing the information would cause material detriment or damage to the data subject, and such data is not sued in decision-making related to the data subject.

Exemption for the right of access (art. 15), the right to rectification (art. 16), the right to restriction of processing (art. 18), the right to data portability (art. 19) and the right to object (art. 21) when processing personal data on the basis of art. 6, 1, (c) of the GDPR (*i.e.* legal obligation) and in accordance with art. 89, 3 of the GDPR. Exemptions also possible in case of processing for the purposes of archiving in the public interest and scientific or historical purposes.

Restrictions to data subject rights

The right of access (art. 15) may be restricted if:

1) providing access to the data could compromise national security, defence or public order or security, or hinder the prevention or investigation of crime;
2) providing access to the data would cause serious danger to the health or treatment of the data subject or to the rights of someone else; or
3) the personal data is used to carry out a monitoring or inspection function, and restricting access to the information is indispensable in order to safeguard an important economic interest of Finland or the EU. The data subject can obtain partial access to the data under specific conditions.

Controller and processor – DPIA and DPO

A DPIA and DPO are required when processing sensitive personal data for a number of purposes, including for scientific and historical research, and statistical purposes. DPO's are subject to general secrecy obligations.

Processing for scientific research purposes

[112] The national GDPR implementation of Finland can be consulted on: https://www.finlex.fi/en/laki/kaannokset/2018/en20181050.pdf (last consulted on 23 September 2020).

Personal data may be processed on the basis of art. 6, 1 (e) of the GDPR (*i.e.* task carried out in the public interest) if it is necessary for scientific or historical research purposes or for statistical purposes and it is proportionate to the public interest pursued.

4.6.5 France[113]

Personal data of deceased persons

Any person may define general or particular guidelines regarding retention, deletion and communication of his/her personal data after death. Personal data of deceased persons may be processed unless the data subject expressed his/her refusal during his/her lifetime.

Age of consent for ISS

A child must be a minimum of 15 years old to give their consent to processing in relation to ISS.

Sensitive personal data

The DPA provides guidance and rules on ensuring the security of processing and to regulate the processing of genetic, biometric and health data. Express consent of the data subject must be obtained in case of processing for medical research purposes involving the examination of genetic characteristics. Health data providers must hold a certificate of conformity from an accredited certifying body in the EU to process personal data for these purposes.

Restrictions to data subject rights

Specific restrictions to data subject rights, for example where personal data are retained in a form which clearly prevents any risk that the data subject may be identified, and where the data is retained for no longer than is necessary for the sole purpose of compiling statistics or carrying out scientific or historical research, under certain conditions.

Controller and processor – DPIA and DPO

A DPA is mandatory in specific cases, for example in case of processing of genetic data of vulnerable persons (*e.g.* patients, employees, children, etc.) and large-scale processing of location data.

International data transfers

Public registers are considered to be national treasures and cannot be transferred outside of French territory.

4.6.6 Germany[114]

Age of consent for ISS

A child must be a minimum of 16 years old to give their consent to processing in relation to ISS.

Sensitive personal data

The processing of genetic, biometric, and health data is subject to additional requirements, for example the processing of genetic data for examination or analysis is only permitted if the data subject has given explicit and written consent.

Exemptions to data subject rights

[113] The national GDPR implementation of France can be consulted on: https://www.legifrance.gouv.fr/loda/id/JORFTEXT000037085952/2020-09-10/ (last consulted on 23 September 2020).

[114] The national GDPR implementation of Germany can be consulted on: https://www.gesetze-im-internet.de/englisch_bdsg/englisch_bdsg.html (last consulted on 23 September 2020).

Where non-automated processing has been carried out, a data subject cannot exercise the right to erasure (art. 17) if:

1) erasure would be impossible or would involve a disproportionate effort due to the specific mode of storage;
2) the data subject's interest in erasure can be regarded as minimal; and 3) the personal data have not been unlawfully processed.

The right to information (art. 14) does not apply if providing information:

1) would threaten public security or public order, or otherwise be detrimental to Germany or a federal state;
2) would interfere with the establishment, exercise or defence of legal claims (unless there is an overriding legitimate interest);
3) the processing includes personal data from private law contracts and is intended to prevent harm from criminal offences (unless overriding legitimate interest); or
4) would disclose information which, by its nature, must be kept secret.

Restrictions to data subject rights

The right to information (art. 13 (3)) does not apply in case:

1) providing information would interfere with the establishment, exercise or defence of legal claims, and the controller's interests in not providing the information outweigh the interests of the data subject;
1) providing information would endanger a confidential transfer of data to public bodies;
2) of further processing of data stored in analogue form, for which the controller directly contacts the data subject through the further processing; the communication with the data subject does not take place in digital form; and the interest of the data subject in receiving the information can be regarded as minimal; or
3) if providing information would endanger public security or order, or would otherwise be detrimental to the welfare of Germany or a federal state.

The right of access (art. 15) does not apply in case:

1) granting access to the personal data would disclose information which, by law or by its nature, must be kept secret;
2) the personal data were recorded only because retention of the relevant personal data is required to comply with applicable law, and disclosure would require disproportionate effort;
3) the personal data is processed to monitor compliance with data protection law or to safeguard other personal data, and disclosure would require disproportionate effort;
4) disclosure is likely to render impossible or seriously impair processing for research or statistical purposes; and
5) the data are necessary for purposes of scientific research, and disclosure would involve disproportionate effort.

The right to rectification (art. 16) does not apply in case:

1) it is likely to render impossible or seriously hinder processing for research or statistical purposes, and limiting the exercise of the right is necessary for the fulfilment of the research or statistical purposes; and
2) it is likely to render impossible or seriously impair processing for archiving purposes in the public interest and limiting the exercise of this right is necessary to fulfil those purposes.

The right to restriction of processing (art. 18) does not apply if it is likely to render impossible or seriously impair processing for archiving purposes in the public interest or for research and statistical purposes, and limiting the exercise of this right is necessary to fulfil those purposes.

The right to data portability (art. 20) does not apply if it is likely to render impossible or seriously impair processing for archiving purposes in the public interest and limiting the exercise of this right is necessary to fulfil those purposes.

The right to object (art. 21) does not apply in case:

1) it is likely to render impossible or seriously hinder processing for research or statistical purposes, and limiting the exercise of this right is necessary for the fulfilment of the research or statistical purpose; and
2) if it is likely to render impossible or seriously hinder processing for archiving purposes in the public interest and limiting the exercise of this right is necessary to fulfil those purposes.

Controller and processor – DPIA and DPO

A DPO must be designated in case a controller or processor:

1) constantly employs at least 20 persons dealing with the automated processing of personal data;
2) undertakes processing subject to an Impact Assessment pursuant to art. 25 of the GDPR; and
3) commercially processes personal data for the purpose of transferring it (including anonymized transfer), or for the purpose of market or opinion research.

DPO's are bound by secrecy when contacted by a data subject, with respect to the identity of the data subject and concerning circumstances enabling the data subject to be identified, unless the DPO is released from this obligation by the relevant data subject.

4.6.7 Italy[115]

Personal data of deceased persons

The data subject rights of articles 15-22 of the GDPR may be exercised with respect to deceased persons by a person who has an interest of his or her own or is acting as a representative to safeguard the deceased person or their family's interests. The exercise of such rights is not permitted where the data subject has expressly refused consent to the processing of his or her personal data.

Age of consent for ISS

A child must be a minimum of 14 years old to give their consent to processing in relation to ISS.

Sensitive personal data

The processing of genetic, biometric, and health data must be done in accordance with specific safeguards adopted by the DPA, taking into account:

1) guidelines and best practices published by the EDPB;
2) scientific and technological developments in the relevant sector; and
3) the principle of free movement of personal data in the EU.

Dissemination of these types of data is prohibited.

Exemptions to data subject rights

Under the rules regarding processing of personal data for statistical purposes in the context of the National Statistics System, statistical and scientific research purposes, where the personal data have not been obtained directly from the data subject, and the provision of the information under art. 14

[115] The national GDPR implementation of Italy can be consulted on: https://www.gpdp.it/documents/10160/0/Codice+in+materia+di+protezione+dei+dati+personali+%28Testo+coordinato%29.pdf/b1787d6b-6bce-07da-a38f-3742e3888c1d?version=1.6 (last consulted on 23 September 2020).

of the GDPR would be particularly burdensome, the controller may use alternative means such as publication of the necessary information in a newspaper or on television.

Restrictions to data subject rights

The rights under art. 15-22 and 77 of the GDPR may not be exercised if it would result in material damage to, for example, the interests protected under the provisions on money laundering.

Controller and processor – DPIA and DPO

Processing of health data can take place without the data subject's consent for the purposes of medical research, subject to appropriate safeguards and an Impact Assessment.

Processing for scientific research purposes

Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes may continue for a longer period than the period for which those data were necessary in relation to the purpose for which they were originally collected. With respect to the processing of sensitive personal data for scientific research or statistical purposes, when the processing is not necessary for reasons of substantial public interest, consent can be obtained from data subjects in a simplified written form. Processing of health data can take place without the data subject's consent, for the purposes of medical research, subject to appropriate safeguards and an Impact Assessment.

4.6.8 Netherlands[116]

Age of consent for ISS

A child must be a minimum of 16 years old to give their consent to processing in relation to ISS.

Sensitive personal data

Based on the legal ground of a substantial public interest (art. 9, 2 (g) GDPR), the processing of genetic data is permitted if the processing takes place with regard to the data subject from whom the relevant data were obtained.

The processing of genetic data is also permitted where, for example, a significant overriding medical reason exists, or the processing is necessary for scientific research purposes in the public interest or statistical purposes.

Based on the legal ground of a substantial public interest (art. 9, 2 (g) GDPR), the processing of biometric data for the unique identification of an individual is permitted if it is necessary for authentication or security purposes.

Based on the legal ground of obligations in the field of employment, social security, and social protection law (art. 9, 2 (b) GDPR), a substantial public interest (art. 9, 2 (g) GDPR), and *e.g.* preventive or occupational medicine (art. 9, 2 (h) GDPR), the processing of health data is permitted by specified actors (*e.g.* employers, pension funds, schools, etc.) and under specific conditions.

Processing for scientific research purposes

Sensitive personal data may be processed for scientific or historical research purposes, or statistical purposes, so long as:

1) the processing is necessary for the scientific or historical research purposes, or statistical purposes in accordance with art. 89 GDPR;
2) the research serves a public interest;
3) it is impossible or would involve a disproportionate effort to request explicit consent; and

[116] The national GDPR implementation of the Netherlands can be consulted on: https://zoek.officielebekendmakingen.nl/stb-2018-144.pdf (last consulted on 23 September 2020).

4) safeguards are in place to ensure that the data subject's privacy is not disproportionately affected.

4.6.9 Portugal[117]

Personal data of deceased persons

The sensitive personal data of deceased persons are protected in accordance with the GDPR and the Data Protection Act. The rights referring to personal data of deceased persons must be exercised by someone appointed by the deceased person for that purpose, or by their heirs. The data subject may decide that the rights in relation to personal data may not be exercised after his or her death.

Age of consent for ISS

A child must be a minimum of 13 years old to give their consent to processing in relation to ISS.

Sensitive personal data

The processing of genetic, biometric, and health data are subject to additional rules:

1) processing of employees' biometric data must only be permitted for the purposes of monitoring attendance and control of access to the employer's facilities, and the employer must ensure that only representations of biometric data are used, and that the data collection procedure does not allow the reverse-identification of such data;
2) health data may only be processed for the purposes of health care, health investigation and other purposes established by law;
3) health data may only be processed in accordance with the written consent of the data subject or of their representative;
4) health systems must assure the separation of health and genetic data from other personal data;
5) insurance companies are not permitted to collect or use any kind of genetic data to refuse a life insurance or to set a higher insurance premium
6) hiring new employees cannot depend on the requirement, performance or results of genetic tests; and
7) employers are not permitted to require their employees to perform or disclose results of genetic tests, even with their consent, except when the workplace involves exposure to significant risks and the genetic information is used for the protection of employees' health, provided that the results are exclusively handed to the data subject and their employment situation will not be put into question.

Exemptions to data subject rights

The rights to information (art. 13 and 14) and of access (art. 15) cannot be exercised against a controller or processor that is subject to a duty of secrecy that applies with respect to the data subject.

Restrictions to data subject rights

When personal data are processed for the purposes of archiving in the public interest, scientific or historical research or statistics, the rights of access (art. 15), rectification (art. 16), restriction of processing (art. 18) and the right to object (art. 21) are restricted to the extent necessary, if such rights would make it impossible to achieve, or seriously impair the achievement of, such purposes.

Controller and processor – DPIA and DPO

[117] The national GDPR implementation of Portugal can be consulted on: https://app.parlamento.pt/webutils/docs/doc.pdf?path=6148523063446f764c324679595842774f6a63334e7a637664326c756157357059326c6864476c3259584d7657456c4a535339305a58683062334d76634842734d5449774c56684a53556b755a47396a&fich=ppl120-XIII.doc&Inline=true (last consulted on 23 September 2020).

The DPA has published a list of cases where a DPIA is mandatory. These include, among others:

1) when processing information that emerges from the use of electronic devices which transmit health data through communication networks;
2) when processing sensitive personal data that have not been obtained from the data subject and the conditions of art. 14, 5 (b) of the GDPR are satisfied; and
3) when processing sensitive personal data for the purpose of archiving in the public interest, scientific or historical research purposes or statistical purposes, with the exception of processing activities authorised by law providing for appropriate safeguards for the rights of data subjects.

4.6.10 Spain[118]

Personal data of deceased persons

Certain persons are authorized to exercise the rights of access (art. 15), rectification (art. 16), and erasure (art. 17) with regard to the personal data of a deceased person:

1) relatives or other persons similarly connected to the deceased person, as well as their legal successors (unless expressly prohibited by the deceased person or as established by law);
2) persons or institutions designated by the deceased person for this purpose, in accordance with the instructions received from the deceased person;
3) if the deceased person is a minor, his or her legal representatives; and
4) if the deceased person was disabled, those who have been designated to carry out support functions, insofar as such exercise falls within the scope of said support functions. Additionally, there are also specific rules regarding access to the personal data of deceased persons managed by information society service providers, including profiles on social networks.

Age of consent for ISS

A child must be a minimum of 14 years old to give their consent to processing in relation to ISS.

Sensitive personal data

In order to prevent unlawful discrimination, sensitive personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and sex life or sexual orientation may not be processed based on the data subject's consent. In such cases, the data subject's consent alone will not be sufficient to permit the processing where the main purpose is identifying these elements. This does not prevent processing such data on the other legal grounds contained in art. 9, 2 of the GDPR.

The processing of health data collected for research purposes is subject to additional requirements:

1) it is lawful and compatible to reuse personal data for the purposes of health and biomedical research where consent was obtained for a specific purpose and the data is used for purposes or research areas which are related to the initial purpose. In such a case, data protection information must be provided via the relevant websites and the data subjects must be informed by electronic means of the existence of such information;
2) it is lawful to use pseudonymized data for health research and biomedical research;
3) where the processing is carried out for the purposes of public health and biomedical research:
    - an Impact Assessment must be conducted;
    - the scientific research must follow quality norms and, where applicable, international guidelines on good clinical practice;

[118] The national GDPR implementation of Spain can be consulted on: https://www.boe.es/boe/dias/2018/12/06/pdfs/BOE-A-2018-16673.pdf (last consulted on 23 September 2020).

- measures must be implemented to guarantee that researchers do not have access to the data subject's identification data; and
- a legal representative in the EU must be appointed if the promoter of the clinical study is not established in the EU;

4) the use of pseudonymized personal data for public health research and biomedical research, must previously be submitted to the research entity's ethics committee (or to the DPO where there is no ethics committee).

Exemptions to data subject rights

Where data subject is exercising his or her right to object (art. 21) to the processing of their data for direct marketing purposes, the controller may retain the necessary identification data of the data subject in order to prevent such processing in the future.

Restrictions to data subject rights

The right of access (art. 15), the right to rectification (art. 16), the right to restriction of processing (art. 18), and the right to object (art. 21) the will be limited in case of processing of personal data for the purposes of health research, if:

1) the aforementioned rights are exercised directly with the researchers or research centres that use anonymized or pseudonymized data;
2) the exercise of such rights relates to the results of the research; and
3) the research is carried out in the public interest related to the security of the State, defence, public safety or other important goals of general public interest.

Controller and processor – DPIA and DPO

Generally, the apportionment of liability between joint controllers will be determined in accordance with the activities that each joint controller carries out.

A DPIA is required in case of processing carried out for public health research purposes. A DPO is mandatory in certain cases, for example for society information service providers when they elaborate or create profiles of users of the service on a large scale. There is a general duty of confidentiality on controllers, processors and all persons involved in any stage of the processing.

4.6.11 Sweden[119]

Age of consent for ISS

A child must be a minimum of 13 years old to give their consent to processing in relation to ISS.

Sensitive personal data

Sector-specific legislation is relevant when processing genetic and health data.

Restrictions to data subject rights

The rights to information (art. 13 and 14) and of access (art. 15) will not apply where the controller cannot, in accordance with the law, disclose the relevant personal data to the data subject.

Additionally, the right of access (art. 15) will be restricted where personal data is contained in a "running text" that has not been finalized when the request is made or which constitutes a memo or a similar document. This restriction does not apply if the personal data:

1) has been disclosed to a third party;

[119] The national GDPR implementation of Sweden can be consulted on: https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-2018218-med-kompletterande-bestammelser_sfs-2018-218 (last consulted on 23 September 2020).

2) is processed solely for archival purposes of public interest or statistical purposes; or
3) has been processed for longer than one year as “running text” without being finalized.

4.6.12 United Kingdom[120]

Personal data of deceased persons

Under the Access to Health Records Act 1990, the following rules apply in respect of access to health records (which contains personal data) relating to deceased persons:

1) a person is entitled to access a deceased person's health records only if they are either a personal representative or a person who has a claim resulting from the death;
2) access to a deceased person's health records may not be granted if a patient requested confidentiality whilst they were alive; and
3) disclosure of a deceased person's health data may also not take place if there is a risk of serious harm to an individual, or if records contain information relating to another person.

Age of consent for ISS

A child must be a minimum of 13 years old to give their consent to processing in relation to ISS.

Sensitive personal data

The processing of genetic, biometric, and health data are subject to additional safeguards (*e.g.* appropriate organizational policies, record-keeping, anonymization, pseudonymization, etc.) depending on the specific legal basis and purposes.

Controller and processor – DPIA and DPO

The DPA has published a list of cases where a DPIA is mandatory. These include, among others:

1) processing involving the use of new technologies, or the novel application of existing technologies;
2) any processing of biometric data for the purpose of uniquely identifying an individual; and
3) any processing of genetic data, other than that processed by an individual GP or health professional for the provision of health care direct to the data subject.

Processing for scientific research purposes

Sensitive personal data may be processed for archiving purposes, scientific or historical research purposes, or statistical purposes, so long as:

1) the processing is necessary for archiving purposes, scientific or historical research purposes or statistical purposes;
2) the processing is carried out in accordance with art. 89, 1 of the GDPR (including implementing safeguards to comply with the principle of data minimization); and
3) the processing is in the public interest.

The table below gives an overview of specific national restrictions on consent for sensitive personal data and restrictions on the use of genetic, biometric and health data in general.

Country	Minimum age of consent for ISS[121]	Restrictions on consent for sensitive personal data[122]	Restrictions on genetic, biometric, and health data
Austria	14 years of age	N/A	N/A
Belgium	13 years of age	N/A	The controller (or, where applicable, the processor) must: 1) maintain a list of the categories of persons having access to the personal data, including a description of their role

			in connection with the processing of the data. That list must be disclosed to the competent DPA on request; and 2) make sure that the people designated are bound by a legal, statutory or contractual obligation of confidentiality with regard to the processed personal data.
Bulgaria	14 years of age	N/A	Insurers can have access to health data of insured individuals or individuals applying for insurance in case: 1) they can obtain it from public authorities and third parties for the establishment of an insured event and the damages caused by such event; or 2) before the conclusion of a life insurance contract and during the term of the contract, the insurer is entitled to receive detailed and accurate information about the age, gender, health and financial status of the person whose life, health or physical integrity will be covered by insurance.
Croatia	16 years of age	The processing of genetic data for the purposes of disease prognosis or other health aspects of the data subject is prohibited, even with the data subject's consent, when that processing is undertaken in connection with the execution or performance of life insurance contracts and contracts with "survival-to-certain-age" clauses. The prohibition applies to data subjects entering into such contracts in Croatia, provided the processing is carried out by a controller with establishment in Croatia or by a controller that provides services in Croatia.	Processing of biometric data is permitted in the private sector, if permitted by the law or if necessary for the protection of persons, property, classified information, business secrets, or individual and secure identification of services users, provided that the data subjects' interests do not override the purpose of such processing. When the processing of biometric data is carried out for the purpose of secure identification of service users, data subjects' explicit consent is required as a legal basis for such processing. In general, the provisions of the national GDPR implementation on the processing of biometric data apply to data subjects in the Republic of Croatia if the processing is carried out by a controller with establishment in the Republic of Croatia or providing services in the Republic of Croatia or by a public authority.

[120] The national GDPR implementation of the United Kingdom can be consulted on: https://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpga_20180012_en.pdf (last consulted on 23 September 2020).

[121] 'ISS' is the abbreviation for 'Information Society Service', defined as: "*any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services*" under Article 1, 1, (b) of Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (codification).

[122] Unless otherwise specified in this overview, all sensitive personal data can be processed lawfully if the data subject has provided valid explicit consent. For specific types of sensitive personal data (*e.g.* genetic, biometric, and health data), there may exist additional restrictions based on the country in question.

Cyprus	14 years of age	Genetic and biometric data cannot be processed for the purposes of obtaining medical and life insurance, even if the data subject has consented.	Processing genetic and biometric data for the purposes of obtaining medical and life insurance is prohibited.
Czech Republic	15 years of age	N/A	N/A
Denmark	13 years of age	When personal data (including sensitive personal data) have been processed for the purpose of carrying out statistical or scientific studies of significant importance to society, then the personal data may not subsequently be processed for other than scientific or statistical purposes, even with the consent of the data subject.	The Act on Research Ethics Review of Health Research Projects[123] contains conditions and limitations on the processing of genetic, biometric, and health data.
Estonia	13 years of age	N/A	The Human Genes Research Act[124] sets out rules for the processing of genetic data for the purposes of genetic research and personalized medicine.
Finland	13 years of age	The Workplace Privacy Act[125] lays down restrictions on the processing of personal data in the context of employment. Unnecessary personal data of employees cannot be processed even with the employee's consent.	Additional requirements under the Act on the Secondary Use of Health and Social Data[126] for the secondary use of health data for registered based health research.[127]
France	15 years of age	Restrictions could be introduced on the processing of sensitive personal data for purposes that cannot be based on the data subject's consent, but no such restrictions have been imposed to date.	The DPA provides guidance and rules on ensuring the security of processing and to regulate the processing of genetic, biometric and health data. Express consent of the data subject must be obtained in case of processing for medical research purposes involving the

[123] A 'health research project' is defined as: "*A project that includes trials involving liveborn human individuals, human gametes intended for fertilization, fertilized human eggs, embryonic cells and embryos, tissue, cells and genetic material from humans, embryos etc. or deceased persons. Also included are clinical trials of medicines in humans and clinical trials of medical devices*"; The Act on Research Ethics Review of Health Research Projects can be consulted on https://en.nvk.dk/rules-and-guidelines/act-on-research-ethics-review-of-health-research-projects (last consulted on 24 September 2020).

[124] The Human Genes Research Act can be consulted on https://www.riigiteataja.ee/en/eli/531102013003/consolide (last consulted on 24 September 2020).

[125] The Workplace Privacy Act can be consulted on https://www.finlex.fi/en/laki/kaannokset/2004/en20040759.pdf (last consulted on 24 September 2020).

[126] The Act on the Secondary Use of Health and Social Data can be consulted on https://stm.fi/documents/1271139/1365571/The+Act+on+the+Secondary+Use+of+Health+and+Social+Data/a2bca08c-d067-3e54-45d1-18096de0ed76/The+Act+on+the+Secondary+Use+of+Health+and+Social+Data.pdf (last consulted on 24 September 2020).

[127] The objective of the Act is to enable efficient and secure processing of personal data collected during the provision of social and healthcare as well as personal data collected for the purpose of steering, supervision, researching and collecting statistics on the social and healthcare sector. Even if not originally stored for the following purposes, the Act applies to aforementioned personal data that used for the purposes of statistics, scientific research, development and innovation activities, education, knowledge management, steering and supervision of social and healthcare by authorities, and planning and reporting duties of authorities.

			examination of genetic characteristics. Health data providers must hold a certificate of conformity from an accredited certifying body in the EU to process personal data for these purposes.
Germany	16 years of age	N/A	The processing of genetic, biometric, and health data is subject to additional requirements, for example the processing of genetic data for examination or analysis is only permitted if the data subject has given explicit and written consent.
Greece	15 years of age	The processing of genetic data for health and life insurance purposes is prohibited.	The processing of genetic data for health and life insurance purposes is prohibited.
Hungary	16 years of age	N/A	Specific rules with regard to the protection of genetic data and health data. The Health Data Processing Act lays down rules concerning the processing of health data. The legislation applies to healthcare providers, all members of the healthcare profession and all legal entities that process health data. Different purposes for processing personal data are specified in the legislation, for example, medical diagnosis and medical treatment, epidemiology and occupational health, public health, statistical purposes, scientific research, etc. The legislation also regulates the processing of health data in the national healthcare network's IT system operated by the State, along with several other databases and registers. Specific rules exist on the conditions and purposes of processing genetic data, including which entities are authorized to process such data, the extent to which the right of access applies and the implementation of specific safeguards (*e.g.* the requirement to obtain written consent from data subjects).
Iceland	13 years of age	N/A	N/A

Ireland	16 years of age[128]	N/A	The processing of genetic data for genetic testing purposes requires the explicit consent of the individual under the Disability Act (2005)[129] and must not otherwise be prohibited by law. Consent is interpreted by reference to the GDPR. The Disability Act also prohibits the processing of genetic data in certain circumstances including for the purposes of insurance or a life assurance policy. In addition, reasonable steps must be taken to provide the individual with appropriate information as to the purposes and possible outcomes of the proposed processing and any potential health implications for the individual which become known as a result of the processing. Depending upon the legal basis relied upon for the processing of biometric data, the Data Protection Act (2018)[130] may impose additional requirements such as the requirement to have in place suitable and specific measures to safeguard the fundamental rights and freedoms of data subjects where the processing of biometric data is for the purposes of carrying out its obligations under employment law. The Health Research Regulations[131] require that the controller, who is processing or further processing personal data for health research, implements suitable measures and safeguards to protect the data subject. For example, the controller must ensure that explicit consent has be obtained from data subjects, except in limited circumstances. It is also required that, in certain circumstances, an Impact Assessment is carried out before the processing of personal data for health research purposes. The processing of health data is lawful where it is necessary and proportionate for the purposes of: 1) an insurance policy or life assurance;

[128] 16 years of age for ISS purposes only. May vary up to 18 years of age for non-ISS purposes, depending on the circumstances; the maturity of the child and their level of understanding of the processing.

[129] The Disability Act can be consulted on http://www.irishstatutebook.ie/eli/2005/act/14/enacted/en/html (last consulted on 24 September 2020).

[130] The Data Protection Act can be consulted on http://www.irishstatutebook.ie/eli/2018/act/7/enacted/en/print (last consulted on 24 September 2020).

[131] The Health Research Regulations can be consulted on http://www.irishstatutebook.ie/eli/2018/si/314/made/en/print (last consulted on 24 September 2020).

			2) health insurance or health-related insurance policy; 3) an occupational pension, retirement annuity contract or any other pension arrangement; or 4) the mortgaging of a property. This is subject to the requirement that suitable and specific measures to safeguard the rights and freedoms of data subjects must be implemented.
Italy	14 years of age	Genetic data cannot be processed by an employer for the purposes of establishing employees' or candidates' working capacity, even if that person's consent has been obtained.	The processing of genetic, biometric, and health data must be done in accordance with specific safeguards adopted by the DPA, taking into account: 1) guidelines and best practices published by the EDPB; 2) scientific and technological developments in the relevant sector; and 3) the principle of free movement of personal data in the EU. Dissemination of these types of data is prohibited.
Latvia	13 years of age	N/A	Under the Human Genome Research Law[132], consent is required from any person donating their genetic material. For example, written consent is required where tissue samples are taken from a data subject, to prepare and supplement the description of their state of health or genealogy, to include data in the genome database, for use in genetic research and for statistical purposes, or to transfer any of the aforementioned data to recipients located outside Latvia.
Liechtenstein	16 years of age	N/A	Sector-specific regulations may be relevant when processing genetic, biometric, and health data.
Lithuania	14 years of age	N/A	N/A
Luxembourg	16 years of age	Genetic data cannot be processed even if the data subject's consent has been obtained.	Processing genetic data in the context of employment and insurance is prohibited.

[132] The Human Genome Research Law can be consulted on https://www.dvi.gov.lv/en/legal-acts/human-genome-research-law/ (last consulted on 24 September 2020).

Malta	13 years of age[133]	Requirements for the processing of sensitive personal data by a competent authority for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.	Requirements for the processing of genetic, biometric, and health data by a competent authority for the prevention, detection and prosecution of crime. The controller must consult the DPA where they intend to process genetic, biometric, and health data for statistical or research purposes based on the legal ground of a task carried out in the public interest. Where genetic data, biometric data or health data are processed for research purposes, the DPA will consult a research ethics committee or an institution recognized by the DPA.
Netherlands	16 years of age	N/A	The processing of genetic data is permitted where: 1) a significant overriding medical reason exists; or 2) the processing is necessary for scientific research purposes in the public interest or statistical purposes (under specific conditions). Specific rules for the processing of genetic, biometric, and health data based on the legal ground of obligations in the field of employment, social security, and social protection law (art. 9, 2 (b) GDPR), a substantial public interest (art. 9, 2 (g) GDPR), and *e.g.* preventive or occupational medicine (art. 9, 2 (h) GDPR).
Norway	13 years of age	N/A	N/A
Poland	16 years of age	N/A	Specific rules for the processing of biometric data by the Polish National Bank.
Portugal	13 years of age	Employers are not permitted to process employees' genetic data, even if the data subject's consent has been obtained, except when the workplace involves exposure to significant risks.	The processing of genetic, biometric, and health data are subject to additional rules: 1) processing of employees' biometric data must only be permitted for the purposes of monitoring attendance and control of access to the employer's facilities, and the employer must ensure that only representations of biometric data are used, and that the data collection

[133] 13 years of age for processing by, or on behalf of, an ISS. 16 years of age for processing personal data of students.

			procedure does not allow the reverse-identification of such data; 2) health data may only be processed for the purposes of health care, health investigation and other purposes established by law; 3) health data may only be processed in accordance with the written consent of the data subject or of their representative; 4) health systems must assure the separation of health and genetic data from other personal data; 5) insurance companies are not permitted to collect or use any kind of genetic data to refuse a life insurance or to set a higher insurance premium 6) hiring new employees cannot depend on the requirement, performance or results of genetic tests; and 7) employers are not permitted to require their employees to perform or disclose results of genetic tests, even with their consent, except when the workplace involves exposure to significant risks and the genetic information is used for the protection of employees' health, provided that the results are exclusively handed to the data subject and their employment situation will not be put into question.
Romania	16 years of age	N/A	The processing of genetic, biometric or health data for the purpose of automated decision-making or profiling is permitted with the express consent of the data subject, or if the processing is performed according to express legal provisions, with the establishment of appropriate measures that protect the legitimate rights, freedoms and interests of data subjects.
Slovakia	16 years of age	Certain legislation, such as the Labour Code, may limit the ability of controllers to process sensitive personal data, even if consent has been obtained.	Controllers may process genetic, biometric and health data on the basis of special laws or an international agreement binding on the Slovak Republic which, in fact, may be regarded as the introduction of an additional legal basis for the processing of the aforementioned personal data.
Slovenia	15 years of age	N/A	In the public sector, biometric data can only be processed in accordance with the law for the following purposes, only where such purposes could not be achieved by other means:

			1) ensuring the security of people or assets; 2) ensuring the security of secret data; 3) complying with obligations under international treaties; 4) enforcing border security; 5) identifying missing or dead persons; or 6) ensuring the security of business secrets; In the private sector, processing biometric data is permitted if it is necessary for the following purposes: 1) ensuring the security of people or assets; 2) ensuring the security of secret data; 3) ensuring the security of business secrets; 4) the processing of biometric data is limited to employees and employees of business partners (provided they have been notified in writing in advance); or 5) the processing of customers' biometric data can be carried out only if provided for by the law and if such persons have given their consent; For the processing of biometric data in the private sector, controllers and processors should notify the DPA in advance and the DPA will then decide within two months whether the measures are in compliance with the legislation or not. The processing of biometric data for marketing purposes is prohibited, even when it is carried out in exchange for free services.
Spain	14 years of age	In order to prevent unlawful discrimination, sensitive personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and sex life or sexual orientation may not be processed based on the data subject's consent. In such cases, the data subject's consent alone will not be sufficient to permit the processing where the main purpose is identifying these elements. This does not prevent processing such data on the other legal grounds contained in art. 9, 2 of the GDPR.	The processing of health data collected for research purposes is subject to additional requirements: 1) it is lawful and compatible to reuse personal data for the purposes of health and biomedical research where consent was obtained for a specific purpose and the data is used for purposes or research areas which are related to the initial purpose. In such a case, data protection information must be provided via the relevant websites and the data subjects must be informed by

			electronic means of the existence of such information; 2) it is lawful to use pseudonymized data for health research and biomedical research; 3) where the processing is carried out for the purposes of public health and biomedical research: ○ an Impact Assessment must be conducted; ○ the scientific research must follow quality norms and, where applicable, international guidelines on good clinical practice; ○ measures must be implemented to guarantee that researchers do not have access to the data subject's identification data; and ○ a legal representative in the EU must be appointed if the promoter of the clinical study is not established in the EU; 4) the use of pseudonymized personal data for public health research and biomedical research must previously be submitted to the research entity's ethics committee (or to the DPO where there is no ethics committee).
Sweden	13 years of age	N/A	Sector-specific regulations may be relevant when processing health and genetic data.
United Kingdom	13 years of age	N/A	The processing of genetic, biometric, and health data are subject to additional safeguards (e.g. appropriate organizational policies, record-keeping, anonymization, pseudonymization, etc.) depending on the specific legal basis and purposes.

Table 4 National restrictions

4.7 General GDPR Requirements

Table 5 General GDPR Requirements gives an overview of different requirements of the GDPR, split into requirements for controllers, processors or both, and with indication whether these are more organisational (O) or possibly also technical (T) requirements. Please note, 'in writing' includes also in electronic form.

Organizational (O) or technical (T) requirement	Obligation/Requirement	Additional Information
DP-1 O/T Types of data	Identify the type of data which will be processed	• Personal data, • special category of data, • non-personal data, • anonymous data
DP-2 O Roles	Define roles: Identify who is controller and who processor	see section 4.2.4
DP-2.1 O	IF controller-processor relationship: establish controller-processor agreement in writing	Art. 28 GDPR. Contract may be based on standard contractual clauses. For information on what must be included see section 4.2.5
DP-2.2 O	IF joint controller relationship: establish joint controller agreement and make the essence of the arrangement available to the data subject	Art. 26 GDPR
DP-2.2.1 O	The joint controller agreement should include allocation of respective responsibilities for compliance with the obligations under this Regulation, in particular: • exercising of the rights of the data subject and their respective duties to provide the information • designate a contact point for data subjects.	Should reflect the respective roles and relationships of the joint controllers vis-à-vis the data subjects. The essence of the arrangement shall be made available to the data subject. The data subject may exercise his or her rights under this Regulation in respect of and against each of the controllers. See EDPB Guidelines 7/2020 for more information
Obligations for controllers		
DP-3 O Purpose	Identify the purpose of the data processing	Clarify why the data will be processed
DP-3.1 O Re-use of data	IF data is processed for another purpose AND not based on consent or legislation, controller must make an assessment on whether the processing is	Art. 6(4) GDPR. The controller should take into account:

	compatible with the purpose for which the personal data are initially collected.	• any link between the original purpose and the further processing purpose; • the context in which the personal data have been collected, in particular regarding the relationship between data subjects and controller; • nature of the personal data: special categories of data or criminal convictions; • possible consequences of the further processing for data subjects; • existence of appropriate safeguards, including encryption or pseudonymisation.
DP-4 O Legal Ground	Identify the legal ground of processing	Art. 6 GDPR: possible legal grounds could be: consent, contract, legal obligation, vital interest, public interest or legitimate interest of the controller For KRAKEN is currently assumed that the legal basis for account data will be contract and for content data consent.
DP-4.1 O/T Consent	IF the processing is based on **consent:** the controller must be able to demonstrate that the data subject has consented to processing of his or her personal data	Art. 7 (1) GDPR
DP-4.1.1 O/T	Consent must comply with the requirements of the GDPR	Art. 7 GDPR, see section 4.3.1 for information on valid consent
DP-4.1.2 T/O	Include possibility to check that the person consenting is over 18	Not a GDPR requirement. Member States can decide on the age of consent, which therefore varies, and parents can give consent to the processing of their children's data (art. 8 GDPR). For general use a minimum age of 18 is the simplest solution, also from an ethical point of view to provide that the data subject has a certain autonomy in their decision making.
DP-4.2 O	IF the processing is based on the ground that it is necessary for the purposes of the **legitimate interests pursued by the controller** or by a third party: it must be ensured that the interests are	Art. 6 (1) (f) GDPR Test: 1) Existence of legitimate interest- Is the processing

Legitimate interest	not overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.	really the legitimate interest? 2) Necessity of processing – Is it really necessary to process the data for that interest (is it proportionate, are there other less intrusive possibilities)? 3) Balancing of interests: What is the interest of the data subject (what will be the impact, what are the reasonable expectations of the data subject)?
DP-4.3 O/T	IF special categories of personal data are processed: explicit consent needed	Art. 9 GDPR normally forbids the processing of special categories of data, except if one of the exemptions apply, the most important for KRAKEN probably explicit consent. National legislation might differ
DP-4.4 O	IF the processing is based upon contract: only process the data relevant for the contract	Art. 6 (1) (b) GDPR; performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.
DP-5 O/T	Keep written records of processing activities	Art. 30 Records of processing activities Should include the following information: • Name and contact details of controller, & if applicable: joint controller, controller's representative, data protection officer • Purpose of the processing • Description of the categories of data subjects and the categories of personal data • Categories of recipients to whom the personal data will be disclosed • In case of transfers to third countries: the country/international organization, in certain cases the suitable safeguards • General description of the technical and organizational security measures

DP-5.1 O	Be able to make the written record available to the supervisory authority on request	
DP-6 O/T Data subject rights	Facilitate the exercise of data subject rights	Art. 12 (2) GDPR; art. 23 GDPR: national restrictions possible
DP-6.1 O/T	Establish measures to easily retrieve information in the case an access request or an audit is filed Be able to: - Inform the data subject whether or not personal data concerning him or her are processed - provide a copy of the personal data (usually in electronic form) → also: in a structured, commonly used and machine-readable format (to be able to comply with the right to data transfer) - provide information	Art. 15 GDPR Right of access; Art. 20 Right to data portability; art. 23 GDPR: national restrictions possible. Information should be: regarding: the purposes, categories of data concerned, recipients, storage period, information on the right to request rectification, erasure or restriction of processing, right to lodge a complaint with the supervisory authority, information regarding the source of the personal data and the existence of automated decision-making, in case of data transfers to a third country, information on the appropriate safeguards.
DP-6.2 O/T	Be able to stop the processing of personal data when a data subject request requires it	Art. 21 GDPR Right to object Restrictions and exceptions are possible
DP-6.3 O/T	Be able to rectify the data without undue delay	Art. 16 GDPR Right to rectification
DP-6.4 O/T	Be able to communicate any rectification, erasure or restriction of processing to each recipient to whom the personal data have been disclosed	Art. 19 GDPR Unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it
DP-6.5 O/T	Be able to erase the data without undue delay	Art. 17 GDPR Right to erasure
DP-6.5.1 O/T	IF the data was made public and must be erased due to a data subject request: take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by	Art. 17 (2) GDPR; art. 23 GDPR: national restrictions possible

	such controllers of any links to, or copy or replication of, those personal data.	
DP-6.6 O/T	If automated individual decision-making is used: Make sure the data subject is aware of it, has a possibility to object against it and provide the possibility to include a 'human in the loop'	Art. 22 GDPR; art. 23 GDPR: national restrictions possible
DP-7 O Data Protection Policy	Implement a data protection policy	
DP-8 O/T Information	Provide **information** to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language and in writing.	Art. 12, 13 and 14 GDPR, for more information see section 4.5. Art. 23 GDPR: national restrictions possible
DP-9 O/T Data protection by design	Implement appropriate technical and organisational measures which are designed to implement data-protection principles in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects -	E.g. pseudonymisation, PET Aspects: • state of the art • Cost of implementation • nature, scope, context and purposes of processing • - risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing
DP-10 O/T Data protection by default	Implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed	Only personal data which are necessary for each specific purpose of the processing are processed, especially with regard to: • the amount of personal data collected, • extent of their processing, • period of their storage, • accessibility. Ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.
DP-11 O Data breach	In case of personal data breach which might result in a risk to the rights and freedoms of natural persons: notify without undue delay and if possible, no later than 72 hours after becoming aware of it to the competent supervisory authority.	Art. 33 Notification of a personal data breach to the supervisory authority. The notification has to include at least: description of the nature of the personal data breach including where possible, the categories and

		approximate number of data subjects concerned and the categories and approximate number of personal data records concerned; the name and contact details of the data protection officer or other contact point where more information can be obtained; the likely consequences of the personal data breach; the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects. → Supervisory authorities often provide forms for notification.
DP-11.1 O	Document any personal data breach: the facts relating to the breach, its effects and the remedial actions taken.	Art. 33 (5) GDPR
DP-11.2 O	In case of a personal data breach which might result in a high risk to the rights and freedoms of natural persons, communicate the breach in clear and plain language and without undue delay to the data subject.	Art. 34 GDPR Communication of a personal data breach to the data subject; Art. 23 GDPR: national restrictions possible
DP-12 O DPIA	In case the processing is likely to result in a high risk to the rights and freedoms of natural persons: make a DPIA before the processing. If the result of the DPIA indicates a high risk: consult the supervisory authority	Art. 35 Data protection impact assessment; see more information in section 4.5; Art. 36 Prior consultation.
DP-13 O Using Processor	IF engaging a processor: only use processor providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject	Art. 28 (1)
Obligations for controllers and processors		
DP-14 O/T Security	Establish technical and organizational security measures to deploy in the processing and storage of information	Art. 32 **Security of processing** ensure a level of security appropriate to the risk In assessing the appropriate level of security account shall be
DP-14.1 O/T	Could use pseudonymisation and encryption of personal data	

DP-14.2 O/T	Should be able to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services	taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed; Approved code of conduct or certification mechanism could be an element to demonstrate compliance
DP-14.3 O/T	Should be able to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident	
DP-14.4 O/T	Should have a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.	
DP-14.5 O/T	Should take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law	
DP-15 O DPO	<u>If necessary</u>, designate a data protection officer and publish the contact details of the DPO and communicate them to the supervisory authority	Art. 37, 38. Necessary if: • Required by Union of Member State law; or • the processing is carried out by a public authority or body, except for courts acting in their judicial capacity; or • the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or • the core activities of the controller or the processor consist of processing on a large scale of special categories of data or personal data relating to criminal convictions and offences.
DP-16 O/T Third country Data Transfer	Only transfer personal data to a third country or an international organization if one of the conditions is given and therefore the level of protection guaranteed by the GDPR is not undermined: • transfer is on the basis of an adequacy decision • transfer is subject to appropriate safeguards	Art. 44 – 49 Data transfers outside of the EU

	• transfer is based on biding corporate rules • one of the derogations of art. 49 is applicable	
Obligations for processors		
DP-17 O/T	Provide sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.	Art. 28 (1)
DP-18 O	Don't engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes	Art. 28 (2)
DP-19 O	IF the processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor shall be imposed on that other processor by way of a contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Regulation.	
DP-20 O	Only process data upon instructions of the controller (except required to do so by Union or Member State law)	Art. 29
DP-21 O/T	Keep a written record of all categories of processing activities	Art. 30
DP-22 O	Notify controller in case of a data breach	Art. 33

Table 5 General GDPR Requirements

5 eIDAS Regulation

5.1 General overview

The European Commission proposed on the 4th of June 2012 a Regulation on **e**lectronic **ID**entification and **A**uthentication **S**ervices (eIDAS)[134]. It was officially published in the OJ on 28 of August 2014[135] and entered into force on the 17th of September 2014. The Regulation is applicable since the 1st of July 2016, the same day the eSignature Directive[136] was repealed, though some articles were applicable before or after that date. Since 29.9.2018 the eIDAS Regulation is in its entirety applicable.

The eIDAS Regulation consists of two main parts: one part concerns provisions regarding electronic identification, and another part concerns trust services. The part on trust services of the eIDAS Regulation does not only cover electronic signatures, but also other trust services.

5.2 Electronic identification

The first main part of the eIDAS Regulation (Chapter II) concerns electronic identification. However, with respect to eIDs, the Regulation focuses on the mutual recognition by Member States, whereas the trust services are treated as market services. [137] The part on electronic identity is therefore restricted and provides for the possibility of cross-border use and mutual recognition of existing electronic identity systems for access to online public services, if the electronic identity schemes have been notified to the Commission and fulfil certain requirements.

Notification

For national electronic identification means to be recognized by other Member States to access online services provided by their public sector bodies the national schemes need to be notified. This means that the electronic identification scheme of a Member State is included in a list of notified electronic identification schemes published by the Commission. In order to be eligible to be notified, an electronic identification scheme must fulfil certain conditions and must be accepted by peer-review: It must be issued either by or under a mandate from the notifying Member State, or at least be recognized by the Member State. They must meet the requirements of an assurance level (see next paragraph), must be used to access a public service in the Member State and must meet certain requirements to be interoperable. Furthermore, the notifying Member State and the party issuing the electronic identification means under that scheme must provide certain assurances, and finally, in order to notify the Member State must provide the other Member States a description of the scheme at least six months before the notification. The requirements for the notification itself are listed in art. 9 eIDAS.

Level of Assurance

Levels of Assurance (LoAs) "characterise the degree of confidence in electronic identification means in establishing the identity of a person, thus providing assurance that the person claiming a particular identity is in fact the person to which that identity was assigned". LoAs are used as an indication of the degree of confidence in the system. Different definitions and systems of assurance levels exist,

[134] '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' (OJ L 257/73, 28.8.2014).

[135] Official Journal of the European Union, L 257/73, 28.8.2014, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:JOL_2014_257_R_0002&from=EN

[136] 'Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures' (OJ L 13/12, 19.1.2000).

[137] Graux, Hans, 'STORK 2.0 D3.1 Legal Needs Analysis Report', 8.5.2013, 23.

resulting from projects such as the STORK project[138], and different standardisation activities. Mainly based upon the results of the STORK project and on the ISO standard 29115, the eIDAS Regulation defines three levels of LoA in article 8 eIDAS Regulation. When Member States notify to the Commission their electronic identity schemes, they must indicate the LoA of the notified scheme. Three levels are defined: low, substantial and high. LoA 'low' indicates identification means which only provide a limited degree of confidence, and the specifications, standards, procedures and controls have the purpose to decrease the risk of misuse or alteration of the identity. 'Substantial' refers to identification means which provide a substantial degree of confidence, and the specifications, standards and procedures intend to decrease the risk of misuse or alteration of the identity substantially. The LoA 'high' finally refers to identification means which provide a higher degree of confidence than identification means with the LoA 'substantial', and the purpose of the technical specifications, standard, procedures and technical controls is to prevent misuse or alteration of the identity. The Commission issued an Implementing Regulation on assurance levels. The Implementing Regulation sets specifications and procedures in its Annex for determining the three different levels. This is done by considering not only the reliability and quality of the enrolment but also the electronic identification means management and the authentication itself. Furthermore, the general management and organisation of participants which provide a service related to electronic identification in a cross-border context, is considered in assessing the assurance level.

5.3 Trust services

It is important to consider that the Regulation does not apply to "the provision of trust services that are used exclusively within closed systems resulting from national law or from agreements between a defined set of participants" (art. 2 (2) eIDAS), which means that for example in case of private blockchain the Regulation might in some cases not be applicable. Of course, it can be agreed between the participants to consider the provisions of the eIDAS Regulation as binding.

The trust services mentioned in the Regulation form a closed list.[139] This means that the provisions of the eIDAS Regulation only apply to the trust services included in the list, though Member States can always nationally recognize additional trust services[140]. The eIDAS Regulation "establishes a legal framework for electronic signatures, electronic seals, electronic time stamps, electronic documents, electronic registered delivery services and certificate services for website authentication."[141]

Trust service is defined as "an electronic service normally provided for remuneration which consists of:

> (a) the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or
>
> (b) the creation, verification and validation of certificates for website authentication; or
>
> (c) the preservation of electronic signatures, seals or certificates related to those services;"[142]

[138] STORK and STORK2.0 were pan-European Project fostering citizens' and business mobility in Europe through cross-border authentication and identification (eID). For more information about STORK and STORK2.0 see e.g. https://ec.europa.eu/digital-single-market/en/content/stork-take-your-e-identity-you-everywhere-eu, http://www.eid-stork.eu/; https://ec.europa.eu/digital-single-market/en/news/end-stork-20-major-achievements-making-access-mobility-eu-smarter;

[139] Recital 25 eIDAS Regulation.

[140] E.g. Belgium recognizes electronic archiving services.

[141] Art. 1 (c) eIDAS Regulation.

[142] Art. 3 (16) eIDAS Regulation.

The eIDAS Regulation defines legal effects for the following trust services:

Trust Service	Legal effect
Electronic signature	Art. 25 (1) eIDAS An electronic signature shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements for qualified electronic signatures.
Advanced electronic signature	Art. 25 (1) eIDAS An electronic signature shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements for qualified electronic signatures.
Qualified electronic signature	Art. 25 (2) eIDAS qualified electronic signature shall have the equivalent legal effect of a handwritten signature
Electronic seal	Art. 35 (1) eIDAS An electronic seal shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements for qualified electronic seals.
Advanced electronic seal	Art. 35 (1) eIDAS An electronic seal shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements for qualified electronic seals.
Qualified electronic seal	Art. 35 (2) eIDAS qualified electronic seal shall enjoy the presumption of integrity of the data and of correctness of the origin of that data to which the qualified electronic seal is linked.
Electronic time stamp	Art. 41 (1) eIDAS An electronic time stamp shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements of the qualified electronic time stamp.
Qualified electronic time stamp	Art. 41 (2) eIDAS A qualified electronic time stamp shall enjoy the presumption of the accuracy of the date and the time it indicates and the integrity of the data to which the date and time are bound.
Electronic registered delivery service	Art. 43 (1) eIDAS Data sent and received using an electronic registered delivery service shall not be denied legal effect and admissibility as evidence

	in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements of the qualified electronic registered delivery service.
Qualified electronic registered delivery service	Art. 43 (2) eIDAS Data sent and received using a qualified electronic registered delivery service shall enjoy the presumption of the integrity of the data, the sending of that data by the identified sender, its receipt by the identified addressee and the accuracy of the date and time of sending and receipt indicated by the qualified electronic registered delivery service.
Website authentication	*No legal effect defined in the eIDAS regulation*
Electronic documents (not a trust service)	Art. 46 eIDAS An electronic document shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in electronic form.

Table 6 Trust services and their legal effects

5.3.1 Special focus: electronic signatures

Within the legal order, signatures fulfil an essential role[143], whereby the act of signing a document can have different functions, such as identifying the signatory, closing the document, and expressing the intention of the signatory. [144] The eIDAS Regulation defines three different types of electronic signatures. Those three types are 'electronic signatures', 'advanced electronic signatures' and 'qualified electronic signatures'[145].

5.3.1.1 Electronic signature

In the eIDAS Regulation the definition of electronic signature reads as 'data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign', which is very similar to the definition in the eSignature Directive. However, the Directive still stated that electronic signatures serve as a method of authentication, which, due to the various

[143] P. van Eecke, "De handtekening in het recht – van pennentrek tot elektronische handtekening", Larcier, Gent, 2004, p.268.

[144] In Germany seven functions are described: Closure function, perpetuation function, identity function, further the signature proves that the information on the document is from the signatory (authenticity function), that the signature is genuine (verification function), it provides evidence (evidence function) and through the conscious act of signing the signatory will be alerted of the legally binding function of the signature (warning function). It has been stressed that an electronic signature needs to be able to fulfil all these requirements in order to be equivalent to a handwritten signature (see BT 14/4987, Gesetzentwurf der Bundesregierung, „Entwurf eines Gesetzes zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsgeschäftsverkehr", 14.12.2000). In Belgium a signature is in general considered to have two functions (identification and the expression of the intention of the signatory), see P. van Eecke, "De handtekening in het recht – van pennentrek tot elektronische handtekening", Larcier, Gent, 2004, p. 191. Patrick van Eecke identifies in his book two additional functions: the security function and the ritual/ceremonial function.

[145] Qualified electronic signatures were not termed as such, but as "advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device". However, the literature generally used the term 'qualified electronic signature', which was also used in the national implementation of the Directive in certain countries (e.g. Germany). The term has now been taken up in the eIDAS Regulation.

meanings of authentication resulted in some confusion regarding the applicability, while the Regulation clarifies that the function of the electronic signature is the signing function.[146]

5.3.1.2 Advanced electronic signature

The 'advanced electronic signature' in the Regulation is an electronic signature which meets all of the following requirements:

- Uniquely linked to the signatory
- Capable of identifying the signatory
- Created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control
- Linked to the data signed therewith in such a way that any subsequent change in the data is detectable

The requirements of the Regulation are slightly less strict than the Directive, as the Directive required a creation with means that the signatory can maintain under his sole control, while the Regulation only requires a high level of confidence.[147] Nevertheless, also the eIDAS Regulation points out the importance of keeping the signature creation data under the sole control of the signatory.

The Commission defined specifications relating to formats of advanced electronic signatures and advanced seals to be recognized by public sector bodies in a Commission Implementing Decision.[148] If a signature meets the standards, which are referenced by the Commission, it can be assumed that the signature fulfils the requirements of an advanced electronic signature.[149]

5.3.1.3 Qualified electronic signature

While the eSignature Directive did not use the term 'qualified electronic signature' as such, the Regulation does use this term to refer to an advanced electronic signature which fulfils some additional requirements. These requirements are:

- It is created using a qualified electronic signature creation device
- based on a qualified certificate for electronic signatures.[150]

Figure 1 gives an overview of all requirements for a qualified electronic signature:

[146] Art. 3 (10) Regulation (EU) 910/2014.
[147] A. Roßnagel, "Neue Regeln für sichere elektronische Transaktionen: Die EU-Verordnung über elektronische Identifizierung und Vertrauensdienste, NJW 2014, 3686", p. 3689, and C. Seegebarth, Perspektiven aus der eIDAS-Verordnung, DuD, 10, 2014, p. 677.
[148] Art. 27 (5) Regulation (EU) 910/2014. Commission Implementing Decision (EU) 2015/1506 of 8 September 2015, laying down specifications relating to formats of advanced electronic signatures and advanced seals to be recognised by public sector bodies pursuant to Articles 27(5) and 37(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market, OJ L235/37, 9.9.2015.
[149] Art. 27 (4) Regulation (EU) 910/2014.
[150] Art. 3 (12) Regulation (EU) 910/2014.

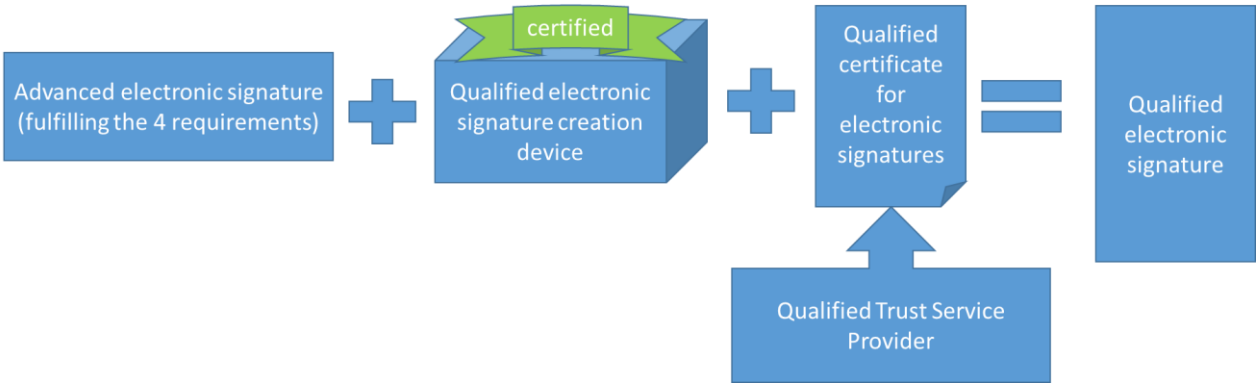


Figure 2 Requirements qualified electronic signature

5.3.1.4 Qualified electronic signature creation device (QESCD)

An electronic signature creation device is software or hardware used to create an electronic signature.

In order to be qualified, the electronic signature creation devices must ensure, with regard to the electronic signature creation data:

(1) that the confidentiality of it is reasonably assured,

(2) that the creation data can practically occur only once,

(3) that the creation data with reasonably assurance cannot be derived, and

(4) that the legitimate signatory can reliably protect the electronic signature creation data against use by others.

Other requirements are that it needs to ensure that the electronic signature is reliably protected against forgery by using currently available technology and that the QESCD shall not alter the data to be signed, or prevent such data from being presented to the signatory prior to signing.[151] The European Commission may, by the means of implementing acts, refer to standards for QESCD[152], which it has done in Commission Implementing Decision 2016/650[153] If a QESCD meets these standards, it shall be presumed to be compliant to the above mentioned requirements.

5.3.1.5 Certification of QESCDs

In order to ensure that the requirements are fulfilled and the device is qualified, it needs to be certified by appropriate public or private bodies designated by the Member States.[154] The Commission may adopt delegated acts outlining specific criteria that have to be met by the designated bodies, and shall establish a list of standards for the security assessment of information technology products.[155] The Member States will inform the Commission no later than one month after the certification is concluded about certified QESCD, and also notify the Commission in case the certification is cancelled and QESCD

[151] Art. 29 (1) Regulation (EU) 910/2014 and Annex II.
[152] Art. 29 (2) Regulation (EU) 910/2014.
[153] Commission Implementing Decision (EU) 2016/650 of 25 April 2016 laying down standards for the security assessment of qualified signature and seal creation devices pursuant to Articles 30 (3) and 39 (2) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market, OJ L109/40, 26.4.2016.
[154] Art. 30 (1) Regulation (EU) 910/2014.
[155] Art. 30 (4) and (3) Regulation (EU) 910/2014. Most of the national supervisory bodies use the standards set by the European Telecommunication Standard Institute (ETSI).

are no longer certified.[156] On the basis of this information, the Commission shall establish, publish and maintain a list of certified QESCDs.[157] The legal effect of this list is not stated in the Regulation.[158]

In recital 56 it is further specified that the Regulation does not cover the entire system environment in which a QESCD operates. Only the hardware and system software used to manage and protect the signature creation data, which has been created, stored or processed in the signature creation device, should be certified.[159] Signature creation applications are excluded from the scope of certification.[160]

5.3.1.6 Qualified Trust Service Provider

To be able to issue qualified certificates, the issuing TSP must be qualified.

The requirements for qualified TSPs in the Regulation are listed in art. 24 eIDAS. The main differences to the eSignature Directive are that the requirements to verify the identity, which first only stated 'by appropriate means and in accordance with national law', are made much more explicit by including how exactly the information can be verified[161] (see also the section 'identification of the signer'). Furthermore, the eIDAS Regulation provides specific guidelines on supervision and the cooperation between different national supervisory bodies. Other requirements are for example that QTSPs have to inform the supervisory body of any change in the provision of their qualified trust services and an intention to cease those activities, they have to record relevant information and keep it accessible for an appropriate period of time, including after the activities of the qualified TSP have been ceased[162], they have to have an up-to-date termination plan to ensure continuity of service[163] and they must ensure lawful processing of personal data in accordance with the Data Protection Directive (and starting from 25 May 2018 with the GDPR).

The fulfilment of the requirements of the Regulation, which is necessary for a TSP to be qualified, will be confirmed via a conformity assessment report issued by a conformity assessment body.[164] The report, together with a notification of the intention to provide qualified trust services, must be submitted to the supervisory body.[165] The supervisory body verifies whether the TSP complies with the requirements, and if it does, the supervisory body will grant qualified status to the TSP and inform the national body responsible for establishing, maintaining and publishing national trusted lists.[166] After the qualified status has been indicated in the trusted list, the qualified TSP may start to provide the qualified trust services and may use the EU trust mark to indicate the qualified trust services it provides. The national trusted lists, which provide information on the qualified trust service providers,

[156] Art. 31 (1) Regulation (EU) 910/2014; A.Roßnagel, Neue Regeln für sichere elektronische Transaktionen: Die EU-Verordnung über elektronische Identifizierung und Vertrauensdienste, NJW 2014, 3686, p. 3689.
[157] Art. 31 (2) Regulation (EU) 910/2014.
[158] A.Roßnagel, Neue Regeln für sichere elektronische Transaktionen: Die EU-Verordnung über elektronische Identifizierung und Vertrauensdienste, NJW 2014, 3686, p. 3690.
[159] Recital 56 Regulation (EU) 910/2014.
[160] Recital 56 Regulation (EU) 910/2014.
[161] These are either: by the physical presence of the natural person or of an authorised representative of the legal person; or remotely, using electronic identification means, for which prior to the issuance of the qualified certificate, a physical presence of the natural person or of an authorised representative of the legal person was ensured and which meets the requirements set out in Article 8 with regard to the assurance levels 'substantial' or 'high'; or by means of a certificate of a qualified electronic signature or of a qualified electronic seal issued after verification by physical presence; or by using other identification methods recognised at national level which provide equivalent assurance in terms of reliability to physical presence. The equivalent assurance shall be confirmed by a conformity assessment body, Art. 24 (1) Regulation (EU) 910/2014.
[162] Art. 24 (2) h Regulation (EU) 910/2014.
[163] Art. 24 (2) i Regulation (EU) 910/2014.
[164] A. Roßnagel, Neue Regeln für sichere elektronische Transaktionen: Die EU-Verordnung über elektronische Identifizierung und Vertrauensdienste, NJW 2014, 3686", p. 3689.
[165] Art. 21 (1) Regulation (EU) 910/2014.
[166] Art. 21 (2) Regulation (EU) 910/2014.

are made available in an electronically signed or sealed form suitable for automated processing.[167] The Commission will make the information on this available to the public in a way suitable for automated processing.[168]

5.3.1.7 Qualified certificate for electronic signatures

To sign with a qualified electronic signature, the signatory additionally needs a 'qualified certificate for electronic signatures'. These certificates have to be issued by a qualified Trust Service Provider (TSP) and must meet the requirements listed in Annex I of the eIDAS Regulation.[169] The requirements are largely similar to the requirements for qualified certificates of the eSignature Directive, with some additions. Examples are, that the certificate must now also contain free of charge the location where the advanced electronic signature or advanced electronic seal of the issuing qualified TSP is available; or that the location of the services that can be used to enquire about the validity status of the qualified certificate must be specified in the certificate. If the creation data related to the validation data is located in a qualified electronic signature creation device, it should include an indication of this, which should be at least suitable for automated processing.[170]

The eIDAS Regulation furthermore requires 'a set of data unambiguously representing the QTSP' (Qualified Trust Service Provider, see below) in order to identify the QTSP. This includes at least the Member State in which that provider is established, for a legal person the name and possibly registration number, and for a natural person that person's name.

The Regulation prescribes that no other mandatory requirements shall be imposed upon qualified certificates for electronic signatures than the ones mentioned in the Regulation.[171] However, the Commission may establish reference numbers of standards for qualified certificates for electronic signatures.

In case a qualified certificate is revoked it will lose its validity from the moment of its revocation, which means that signatures made before the revocation are still valid. The QTSP is obliged to register a revocation in its certificate database and publish the revocation status within 24 hours after the receipt of the request. The revocation becomes effective immediately upon its publication.[172]

Another possibility is the temporary suspension of a certificate, however, this would be governed by national rules.[173] Temporary suspension is generally considered problematic, since signatures created within the period of suspension may or may not be valid if the certificate is reinstated after the suspension (suspension with or without obliteration).[174] The eIDAS Regulation provides that Member States may only lay down rules under the condition that the qualified certificate will lose its validity for the period of suspension and that the period of suspension will be clearly indicated in the certificate database.[175] Furthermore, the suspension status during the period of suspension should be visible from the service providing information on the status of the certificate.[176]

---

[167] Art. 22 (1) and (2) Regulation (EU) 910/2014.
[168] Art. 22 (4) Regulation (EU) 910/2014.
[169] A.Roßnagel, Neue Regeln für sichere elektronische Transaktionen: Die EU-Verordnung über elektronische Identifizierung und Vertrauensdienste, NJW 2014, p. 3689.
[170] Annex I (j) Regulation (EU) 910/2014.
[171] Art. 28 (2) Regulation (EU) 910/2014.
[172] Art. 24 (3) Regulation (EU) 910/2014.
[173] See C. Seegebarth, Perspektiven aus der eIDAS Verordnung, DUD 10, 2014, p. 676.
[174] See p. 10 of the study SMART 2012/0001, Phase II - Electronic signatures in public services Version 2.1, 5 June 2014.
[175] Art. 28 (5) Regulation (EU) 910/2014.
[176] Art. 28 (5) Regulation (EU) 910/2014.

5.3.1.8 Identification in certificates

Signatures have an identificatory function. Therefore, this section will look at the identification of the signer under the provisions of the eIDAS Regulation.

Art. 24 eIDAS specifies explicitly that when qualified TSPs issue qualified certificates for a trust service (note that this is generally for trust services, not specifically electronic signatures), they should verify "by appropriate means and in accordance with national law" the identity and also specific attributes of the natural or legal person if applicable. Art. 24 eIDAS furthermore specifies ways to verify, which should be in accordance with national law and can be direct or by relying on a third party. The possibilities of identity verification are:

> 1) by the physical presence of the natural person or of an authorised representative of the legal person; or
>
> 2) remotely, using electronic identification means, for which prior to the issuance of the qualified certificate, a physical presence of the natural person or of an authorised representative of the legal person was ensured and which meets the requirements of the assurance levels 'substantial' or 'high'; or
>
> 3) by means of a certificate of a qualified electronic signature or of a qualified electronic seal issued in compliance with the first two possibilities; or
>
> 4) by using other identification methods recognised at national level which provide equivalent assurance in terms of reliability to physical presence.[177] The equivalent assurance must be confirmed by a conformity assessment body.[178]

Annex I of the eIDAS Regulation provides a list of requirements for qualified certificates for electronic signatures. These certificates are necessary for a qualified electronic signature. The signatory will always be a natural person, since it would otherwise be an electronic seal. Annex I specifies that the name of the signatory should be included in the certificate. It is allowed to use a pseudonym instead of a name, but it must be clearly indicated that a pseudonym is used.[179] It is possible to add non-mandatory additional specific attributes, as long as they don't affect the interoperability and recognition of qualified electronic signatures.[180]

EN 319 412-2 of 2016 (V2.2.1) specifies the certificate profile for certificates issued to natural persons.[181] For the subject field three attributes must be included: **countryName**, **commonName**, and either **givenName** and **surname**, or **pseudonym**.[182] In case those would not ensure uniqueness within the context of the issuer of the certificate, then additional **serialNumber** must be included.[183] It can be a governmental identifier or simply a number or code assigned by the CA.[184] Both **commonName** and **givenName/surname** or **pseudonym** are considered necessary in order to maximise interoperability, whereby **commonName** is for "user friendly representation of the person's

[177] Art. 24 eIDAS Regulation.
[178] Art. 24 (1) (d) eIDAS Regulation.
[179] Annex I (c) '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'.
[180] Art. 28 (3) eIDAS Regulation.
[181] 'ETSI EN 319 412-2 V2.1.1 (2016-02) Electronic Signatures and Infrastructures (ESI);Certificate Profiles; Part 2: Certificate Profile for Certificates Issued to Natural Persons', n.d., 412.
[182] 'ETSI EN 319 412-2 V2.1.1 (2016-02) Electronic Signatures and Infrastructures (ESI);Certificate Profiles; Part 2', 9.
[183] 'ETSI EN 319 412-2 V2.1.1 (2016-02) Electronic Signatures and Infrastructures (ESI);Certificate Profiles; Part 2', 9.
[184] 'ETSI EN 319 412-2 V2.1.1 (2016-02) Electronic Signatures and Infrastructures (ESI);Certificate Profiles; Part 2', 94.2.4 Subject.

name" and **givenName/surname** for a "more formal representation or verification of specific identity of the user"[185].

ETSI EN 319 411-1 is interesting, as the above-mentioned standard defines how the information should be included in a certificate, but not how the information is obtained and verified. ETSI EN 319 411-1 of 2018 includes general requirements for TSPs who issue certificates. In the standard are the different PKI participants considered, whereby for the question of electronic identity especially the subject is interesting, as it is the "entity identified in a certificate as the holder of the private key associated with the public key given in the certificate"[186], and in particular when the subject is a natural person.[187] The requirements for naming are for natural persons specified as explained in the above mentioned standard ETSI EN 319 412 -2, and in ISO/IEC 9594-8/Recommendation ITU-T X.509[188] and in IETF RFC 5280[189].[190]

Depending on the type of certificate, the requirements for identity validation are different. In general it requires that the TSP must verify the identity and the certificate requests, at the time of registration and by appropriate means.[191] The standard further specifies that the TSP must collect either direct evidence or 'an attestation from an appropriate and authorized source' for the identity and, if applicable, any specific attributes.[192] Evidence must be given for the full name, including surname and given names consistent with the national identification practices and, in order to distinguish the person from others with the same name, information such as date and place of birth, reference to a nationally recognized identity document, or other attributes which can be used for this purpose.[193] In case the subject is a natural person who is identified in association with a legal person, then additionally evidence is also needed for information on the legal person (e.g. full name and legal status, relevant registration information and the affiliation of the natural person to the legal person).[194] This evidence can be in paper form or in electronic form, but the authenticity of the evidence must be validated.[195]

---

[185] 'ETSI EN 319 412-2 V2.1.1 (2016-02) Electronic Signatures and Infrastructures (ESI);Certificate Profiles; Part 2', 9.

[186] 'ETSI EN 319 411-1 V1.2.2 (2018-04) ETSI EN 319 411-1 V1.2.2 (2018-04)Electronic Signatures and Infrastructures (ESI);Policy and Security Requirements for Trust Service Providers Issuing Certificates;Part 1: General Requirements', n.d., 11.

[187] In the standard are furthermore also a natural person identified in association with a legal person; a legal person; or a device or system operated by or on behalf of a natural or legal person considered as subjects 'ETSI EN 319 411-1 V1.2.2 (2018-04) ETSI EN 319 411-1 V1.2.2 (2018-04)Electronic Signatures and Infrastructures (ESI);Policy and Security Requirements for Trust Service Providers Issuing Certificates;Part 1', 18.

[188] ISO/IEC 9594-8/Recommendation ITU-T X.509: "Information technology - Open Systems Interconnection - The Directory - Part 8: Public-key and attribute certificate frameworks".

[189] IETF RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.

[190] 'ETSI EN 319 411-1 V1.2.2 (2018-04) ETSI EN 319 411-1 V1.2.2 (2018-04)Electronic Signatures and Infrastructures (ESI);Policy and Security Requirements for Trust Service Providers Issuing Certificates;Part 1', 20.

[191] 'ETSI EN 319 411-1 V1.2.2 (2018-04) ETSI EN 319 411-1 V1.2.2 (2018-04)Electronic Signatures and Infrastructures (ESI);Policy and Security Requirements for Trust Service Providers Issuing Certificates;Part 1', 20 and REG-6.2.2-02.

[192] 'ETSI EN 319 411-1 V1.2.2 (2018-04) ETSI EN 319 411-1 V1.2.2 (2018-04)Electronic Signatures and Infrastructures (ESI);Policy and Security Requirements for Trust Service Providers Issuing Certificates;Part 1', 20 REG-6.2.2-02.

[193] 'ETSI EN 319 411-1 V1.2.2 (2018-04) ETSI EN 319 411-1 V1.2.2 (2018-04)Electronic Signatures and Infrastructures (ESI);Policy and Security Requirements for Trust Service Providers Issuing Certificates;Part 1', 21 REG-6.2.2-06.

[194] 'ETSI EN 319 411-1 V1.2.2 (2018-04) ETSI EN 319 411-1 V1.2.2 (2018-04)Electronic Signatures and Infrastructures (ESI);Policy and Security Requirements for Trust Service Providers Issuing Certificates;Part 1', 21 REG-6.2.2-09.

[195] 'ETSI EN 319 411-1 V1.2.2 (2018-04) ETSI EN 319 411-1 V1.2.2 (2018-04)Electronic Signatures and Infrastructures (ESI);Policy and Security Requirements for Trust Service Providers Issuing Certificates;Part 1', 20 REG-6.2.2-02.

This evidence must be checked against the natural person either directly or indirectly.[196] Directly means checking it by the physical presence of the person, while with indirectly checking the means must provide equivalent assurance as the physical presence, such as for example if the evidence is electronically signed by a trusted party.[197] For TSPs issuing qualified certificates is in ETSI EN 319 411-2 a bit more specific explained that the same requirements as in ETSI EN 319 411-1 apply, and in addition that, when the verification is indirectly, the methods used should provide "equivalent assurance in terms of reliability to the physical presence" and the TSP should be able to prove the equivalence.[198] This proof of equivalence can be done according to the eIDAS Regulation[199] and it is specially noted that it needs to consider the impersonation risks.[200] This risk can be increased by a chain of remote registrations as the connection to the original face to face verification is weakened and it makes it possible to receive documents without the person being seen for years.[201]

With regards to the identification of the signer two aspects are important: which information must be provided, and how is the information verified upon registration? The eIDAS Regulation itself only specifies that the name of the signatory or a clearly indicated pseudonym must be included in the certificate, and additional attributes may be included. In the standards more detailed information is provided. ETSI EN 319 412-2 specifies that for certificates issued to natural persons normally three attributes should be included: the country name, common name and either the official given name and surname or a pseudonym. In case this is not unique, than additionally a serial number must be included which can be either provided by the TSP or can be a governmental identifier such as a passport number or a national unique identification number. The information must normally be provided by the requester of the certificate, the natural person. The TSP must verify that the provided information is indeed correct. This should be done by appropriate means and in accordance with national law, and four possibilities are given in art. 24 eIDAS: the first possibility is verification by physical presence of the natural person, the second is by electronic identification with electronic identification means with a level of assurance substantial or high, the third possibility is the use of a certificate of a qualified electronic signature or qualified electronic seal, and the last possibility is to use reliable national recognised identification methods. The third possibility shows that it is allowed to use an electronic signature certificate as authentication means, if it is qualified.

5.4 SSI and eIDAS

The idea of self-sovereign identity (SSI) is, that the user can create and manage their identity individually, often using distributed ledger technologies (e.g. blockchain), without the necessity of involving a third party.[202] SSI is often using an identifier, the so called "decentralized identifier" (DID).

---

[196] 'ETSI EN 319 411-1 V1.2.2 (2018-04) ETSI EN 319 411-1 V1.2.2 (2018-04)Electronic Signatures and Infrastructures (ESI);Policy and Security Requirements for Trust Service Providers Issuing Certificates;Part 1', 20 REG-6.2.2.-05.

[197] 'ETSI EN 319 411-1 V1.2.2 (2018-04) ETSI EN 319 411-1 V1.2.2 (2018-04)Electronic Signatures and Infrastructures (ESI);Policy and Security Requirements for Trust Service Providers Issuing Certificates;Part 1', 20 REG-6.2.2.-05.

[198] 'ETSI EN 319 412-2 V2.1.1 (2016-02) Electronic Signatures and Infrastructures (ESI);Certificate Profiles; Part 2', 14 REG-6.2.2-02.

[199] See art. 24 (1) (d) eIDAS Regulation.

[200] 'ETSI EN 319 412-2 V2.1.1 (2016-02) Electronic Signatures and Infrastructures (ESI);Certificate Profiles; Part 2', 14 REG-6.2.2-02.

[201] 'ETSI EN 319 412-2 V2.1.1 (2016-02) Electronic Signatures and Infrastructures (ESI);Certificate Profiles; Part 2', 14 REG-6.2.2-02.

[202] Ignacio Alamillo Domingo, 'SSI EIDAS Legal Report - How EIDAS Can Legally Support Digital Identity and Trustworthy DLT-Based Transactions in the Digital Single Market', April 2020, 13.

This identifier is a "portable URL-based identifier" which is associated with an entity.[203] DIDs can resolve to DID documents.[204] A DID document includes a set of data which is associated with the DID, and can include information that the person who the DID identifies can use to authenticate itself.[205] DIDs can be recorded in a verifiable data registry (e.g. on a distributed ledger).[206] This entity using SSI to authenticate itself can be a natural person, though it might also be a legal person. In case the DID is from a natural person it means it will normally 'relate to an identified or identifiable person' and therefore most likely be personal data. For the eIDAS Regulation it will depend upon how the DID will be used.

5.4.1 SSI in KRAKEN

In KRAKEN are at the current moment four ideas envisaged (forthcoming deliverable D2.2 v1.2. section 4.4.10. v1.2):

The first one is to create a verifiable credential. The objective in this case is the creation of an Identity Verifiable Credential which would be based on the national digital identity of the holder.[207] The holder would use an Identity Broker (the 'LegalIdentityManager (LIM)) which acts as an issuer and who would, after the authentication of the holder with the national authentication means, would issue and sign an Identity Verifiable Credential with the obtained information.[208]

The second idea is to create an eIDAS signature certificate. The objective of this process is to create, based upon an existing Verifiable Credential, for example one obtained during the first process, a keypair and a digital signature certificate.[209] The LIM would in this case act as a verifier.[210] The LIM would generate a signature key pair for the holder of the Verifiable Credential and store the private key on a Hardware Security Module (HSM). [211] The LIM will furthermore act as a Registration Authority and submit to the Certification Authority a request for a certificate (advanced or qualified) for the public key of the generated key pair, which will be stored by the LIM service. Afterwards the holder could use the LIM service as a remote signature service. [212]

The third idea is to issue eIDAS –signed/sealed verifiable credentials. The objective of this process is that the issuer can create verifiable credentials which are signed or sealed with an eIDAS signature/seal.[213] The idea in this case is that not the whole credential is signed but instead every single attribute is separately signed.

The fourth idea is a validation of eIDAS signed Verifiable Credentials. The objective of this process is to validate a Verifiable Credential which was signed with an eIDAS signature (or seal).[214] It is planned that the LIM will implement the validation of eIDAS-signed attributes and can be used for this by any service (verifier).[215]

[203] Domingo, 93.
[204] https://w3c.github.io/did-core/.
[205] https://w3c.github.io/did-core/; https://w3c.github.io/did-core/#dfn-did-documents .
[206] https://w3c.github.io/did-core/ .
[207] KRAKEN D2.2 section 4.4.10.1., v1.2, p.45.
[208] KRAKEN D2.2 section 4.4.10.1., v1.2, p.45.
[209] KRAKEN D2.2 section 4.4.10.2., v1.2, p.46.
[210] KRAKEN D2.2 section 4.4.10.2., v1.2, p.46.
[211] KRAKEN D2.2 section 4.4.10.2., v1.2, p.46.
[212] KRAKEN D2.2 section 4.4.10.2., v1.2, p.46.
[213] KRAKEN D2.2 section 4.4.10.3., v1.2, p.47.
[214] KRAKEN D2.2 section 4.4.10.4., v1.2, p.48.
[215] KRAKEN D2.2 section 4.4.10.4., v1.2, p.48.

5.4.2 Analysis eIDAS – KRAKEN SSI options

5.4.2.1 Create a verifiable credential on the basis of a national digital identity

As explained before, with regard to electronic identification, the Regulation focuses on mutual recognition by Member States. The eIDAS Regulation focuses on the possibility of cross-border use and mutual recognition of existing electronic identity systems for access to online public services. To be accepted by the online public services, the electronic identity schemes have been notified to the Commission, fulfil certain requirements and are therefore accepted during peer-review. Member States are, however, neither obliged to have a national electronic identification scheme nor to notify their national electronic identification scheme if they have one. There is also no obligation to allow the use of their authentication possibility by the private sector.[216] Nevertheless, the eIDAS Regulation provides that "the authentication possibility provided by any Member State should be available to private sector relying parties established outside of the territory of that Member State under the same conditions as applied to private sector relying parties established within that Member State. Consequently, with regard to private sector relying parties, the notifying Member State may define terms of access to the authentication means. Such terms of access may inform whether the authentication means related to the notified scheme is presently available to private sector relying parties."[217]

As explained earlier, when Member States notify to the Commission their electronic identity schemes, they must indicate the LoA of the notified scheme. The three levels are: low, substantial and high. Only eID means with the LoA substantial and high must be accepted by online public services. Deriving a Verifiable Credential from notified eID means with a substantial or high LoA therefore implies that the attributes are more trustworthy. However, this does not mean that the Verifiable Credential has the same LoA as the eID means from which the information was derived.

Open Questions:

1) *Do the national eID schemes allow private sector parties the use of their eIDs?*
2) *What will be the LoA of the Verified Credential?*

5.4.2.2 Create an eIDAS signature certificate based upon a Verifiable Credential

The aim is that the resulting electronic signature is either an advanced or a qualified electronic signature.

Requirements for an advanced electronic signature:

- Uniquely linked to the signatory
- Capable of identifying the signatory
- Created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control
- Linked to the data signed therewith in such a way that any subsequent change in the data is detectable

[216] Recital 17 eIDAS Regulation.
[217] Recital 17 eIDAS Regulation.

Previously the e-Signature Directive required a creation with means that the signatory can maintain under his sole control. The Regulation only requires a high level of confidence, which was adjusted in order to allow for remote signature services using HSMs.[218]

The requirements for an advanced electronic seal are the same just applied to a seal, e.g. the 'signer' is replaced with 'creator of the seal' and 'electronic signature creation data' is 'electronic seal creation data'.[219]

As long as the requirements are fulfilled (e.g. key pair must be secure and only be used by the signer and the signer must be identifiable) it should be no problem to obtain a certificate for the key pair and create advanced electronic signatures or seals, also remotely.

Requirements for a qualified electronic signature:

- Uniquely linked to the signatory
- Capable of identifying the signatory
- Created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control
- Linked to the data signed therewith in such a way that any subsequent change in the data is detectable
- It is created using a qualified electronic signature creation device
- based on a qualified certificate for electronic signatures

The first four requirements are the ones for an advanced electronic signature.

The requirement for using a qualified electronic signature creation device means that in case an HSM will be used, this HSM must fulfil the requirements for a qualified electronic signature creation device and must be certified. The European Commission maintains a list of certified QESCDs, based upon national information.[220]

The requirement that is must be based on a qualified electronic certificate for electronic signatures means that the electronic signature certificate which would be created based upon a Verifiable Credential would need to fulfil certain requirements.

1) It must be issued by a qualified Trust Service Provider (in case of KRAKEN e.g. Infocert)
2) It must meet the requirements listed in Annex I of the eIDAS Regulation.

The Regulation prescribes that no other mandatory requirements shall be imposed upon qualified certificates for electronic signatures than the ones mentioned in the Regulation.[221] However, the Commission may establish reference numbers of standards for qualified certificates for electronic signatures.

Though of course all requirements of Annex I eIDAS Regulation must be fulfilled, it is worth looking specially into requirement (c) which requires that the qualified certificate shall contain "at least the name of the signatory, or a pseudonym; if a pseudonym is used, it shall be clearly indicated". For qualified electronic seals, which are again very similar to qualified electronic signatures Annex III provides the requirements for qualified certificates for electronic seals, which are largely the same as Annex I, but requirement (c) states that the certificate should contain "at least the name of the creator of the seal and, where applicable, registration number as stated in the official records".

[218] A. Roßnagel, "Neue Regeln für sichere elektronische Transaktionen: Die EU-Verordnung über elektronische Identifizierung und Vertrauensdienste, NJW 2014, 3686", p. 3689, and C. Seegebarth, Perspektiven aus der eIDAS-Verordnung, DuD, 10, 2014, p. 677.
[219] Art. 36 eIDAS Regulation.
[220] https://ec.europa.eu/futurium/en/content/compilation-member-states-notification-sscds-and-qscds .
[221] Art. 28 (2) Regulation (EU) 910/2014.

Art. 24 eIDAS specifies that qualified TSPs must verify "by appropriate means and in accordance with national law" the identity and also specific attributes of the natural or legal person if applicable.

This can be done:

1) by the physical presence of the natural person or of an authorised representative of the legal person; or

2) remotely, using electronic identification means, for which prior to the issuance of the qualified certificate, a physical presence of the natural person or of an authorised representative of the legal person was ensured and which meets the requirements of the assurance levels 'substantial' or 'high'; or

3) by means of a certificate of a qualified electronic signature or of a qualified electronic seal issued in compliance with the first two possibilities; or

4) by using other identification methods recognised at national level which provide equivalent assurance in terms of reliability to physical presence.[222] The equivalent assurance must be confirmed by a conformity assessment body.[223]

This means that either the Verifiable Credential must have an LoA 'substantial' or 'high' and has been issued upon physical presence; or it would need to be already a qualified certificate (double, unlikely); or it would need to be recognized at national level as an identification method and the equivalent assurance must be confirmed by a conformity assessment body.

5.4.2.3 Issuing eIDAS –signed/sealed verifiable credentials

The objective of this process is that the issuer can create verifiable credentials which are signed or sealed with an eIDAS signature/seal.[224] The idea in this case is that not the whole credential is signed but instead every single attribute is separately signed. The advantage of signing with an advanced or qualified electronic signature or seal is the increased trust created by the signature or seal, since these have the legal effects shown in section 5.3. and can be used in legal proceedings as evidence. The requirements for a valid advanced or qualified electronic signature or seal as explained earlier and for the second case must be taken into account.

5.4.2.4 Validation of eIDAS signed Verifiable Credentials

The objective of this process is to validate a Verifiable Credential which was signed with an eIDAS signature (or seal?).[225] It is planned that the LIM will implement the validation of eIDAS-signed attributes and can be used for this by any service (verifier).[226]

The requirements for the validation of qualified electronic signatures are provided in art. 32 eIDAS Regulation. The system which is used to validate the qualified electronic signature shall provide to the relying party the correct result of the validation process and shall allow the relying party to detect any security relevant issues.[227] The validity of a qualified electronic signature shall be confirmed if the certificate was at the time of signing a qualified certificate, valid and issued by a qualified trust service provider. Furthermore, the data provided to the relying party must correspond correctly to the signature validation data as well as the unique set of data representing the signatory in the certificate.

[222] Art. 24 eIDAS Regulation.
[223] Art. 24 (1) (d) eIDAS Regulation.
[224] KRAKEN D2.2 section 5.4.9. v0.6, p.44.
[225] KRAKEN D2.2 section 5.4.9. v0.6, p.45.
[226] KRAKEN D2.2 section 5.4.9. v0.6, p.45.
[227] Art. 32 (2) eIDAS Regulation.

In case a pseudonym was used then it must have been clearly indicated to the relying party. Finally, the requirements for an advanced electronic signature must have been met, the electronic signature must have been created by a qualified electronic signature creation device and the integrity of the signed data must not have been compromised. The Commission may adopt implementing acts which mention reference numbers of standards for the validation of qualified electronic signatures.

As shown in section 5.3., the validation of electronic signatures or electronic seals is a trust service. The entity providing the validation service could then be considered either a normal or a qualified trust service provider, depending whether the requirements for a qualified trust service provider are fulfilled. A qualified trust service provider can also provide a qualified validation service for qualified electronic signatures if it provides validation in compliance with art. 32 (1) eIDAS Regulation and allows the relying parties to receive the result of the validation process in an automated manner, which is reliable, efficient and bears the advanced electronic signature or advanced electronic seal of the provider of the qualified validation service.[228] The requirements for the normal and the qualified validation of qualified electronic signatures apply mutatis mutandis also for the validation of qualified electronic seals.[229]

[228] Art. 33 eIDAS Regulation.
[229] Art. 40 eIDAS Regulation.

6 E-commerce Directive and Platform Regulation

As the KRAKEN service will be a service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of the service, it can be considered an information society service.[230] Therefore, the provisions of the e-Commerce Directive[231] are potentially relevant for KRAKEN. As it is a Directive, the national provisions implementing the Directive would need to be considered in the country where the KRAKEN provider would be located. For the development of the platform the provisions of the Directive will be considered, in order to assess which obligations could potentially be relevant for the development of the KRAKEN system.

Since 12 July 2020 is the Regulation 2019/1150 applicable, on promoting fairness and transparency for business users of online intermediation services. It is not entirely clear whether the Regulation is applicable to KRAKEN. This will depend upon whether the KRAKEN service can be considered an online intermediation service. Online intermediation services are services which are 1) information society services which 2) allow business users to offer goods or services to consumers with a view to facilitating the initiating of direct transactions between those business users and consumers and which 3) are provided to business users on the basis of contractual relationships between the provider of those services and business users which offer goods or services to consumers. It is likely that the data providers might also be businesses, less likely is that the data receivers will be consumers. Nevertheless, since this possibility is also not excluded, the Regulation has been considered in the analysis for requirements. Table 7 gives an overview of the identified requirements:

Requirement	Requirement description	Notes
ECOM-1	Establish whether the user is acting as a consumer or a business user	Relevant to decide which provisions are applicable Consumer: a natural person who is acting for purposes which are outside this person's trade, business, craft or profession (art. 2 (4) Regulation 2019/1150; art. 2 (d) e-Commerce Directive) Business user: any private individual acting in a commercial or professional capacity who, or any legal person which, through online intermediation services offers goods or services to consumers for purposes relating to its trade, business, craft or profession (art. 2 (1) Regulation 2019/1150)

[230] Art. 2 (a) e-Commerce Directive jo. Art. 1 (b) Directive 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services, *OJ* L241/1, 17.9.2015.

[231] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, *OJ* L178/1, 17.7.2000.

ECOM-2	Include easily reachable at least the following information on the UI (e.g. website) • the name of the service provider • the geographic address at which the service provider is established • details of the service provider, including e-mail address • in case of registration in a trade or similar public register: the register and registration number • in case of VAT: tax registration number	Art. 5 e-Commerce Directive
ECOM-3	For the conclusion of a contract with a consumer: provide the following information clearly, comprehensively and unambiguously and prior to the conclusion of the contract: • The different technical steps to follow to conclude the contract; • Whether or not the concluded contract will be filed by the service provider and whether it will be accessible; • The technical means for identifying and correcting input errors prior to the placing of the order; • The languages offered for the conclusion of the contract	Art. 10 (1) e-Commerce Directive
ECOM-4	Terms and conditions • must be made available in a way that allows the user to store and reproduce them; • must be drafted in plain and intelligible language, • easily available to users at all stages of their commercial relationship with KRAKEN, • in case of any changes the users must be notified	Art. 10 (2) e-Commerce Directive Art. 3 (1) and (2) Regulation 2019/115 (in principle only for business users) ➔ selection of requirements for T&Cs that could potentially be relevant for development
ECOM-5	Transfer of content data: KRAKEN should not initiate the transmission, select the receiver of the transmission or select or modify the information contained in the transmission	Art. 12 e-Commerce Directive (‘mere conduit’)
ECOM-6	Content data: KRAKEN should not monitor the data.	Art. 14 e-Commerce Directive
ECOM-6.1.	Upon obtaining knowledge or awareness of illegal activity or information must act expeditiously to remover or to disable access to the information	Art. 14 e-Commerce Directive

ECOM-7	Provide an internal complaint-handling system • easily accessible and free of charge • ensure handling within a reasonable time frame • able to communicate to the complainant the outcome of the internal complaint-handling process in an individualized manner and drafted in plain and intelligible language	Art. 11 Regulation 2019/115 (in principle only for business users)

Table 7 E-commerce requirements

7 General overview Ethics requirements

The law, in particular legislation protecting fundamental rights such as Data protection law, already addresses ethical aspects.[232] Many ethical aspects can therefore already be found in legal provisions.[233] Nevertheless, it is important to look at the broader application and consider whether it is possible to identify guidelines and principles that can be used in the development of KRAKEN, as well as clearly identify the decisions that are made and their possible ethical implications. Most technical requirements which are based upon these considerations have already been included in the list of data protection requirements.

7.1 Introduction

Various methods exist to include ethics into research and innovation. Reijers et al. in their overview of R&I ethics methods divide the methods into ex ante methods, intra methods and ex post methods.[234] In their analysis, Reijers et al. recommend that during the development the focus should be more on the integration of ethics in the daily work of the researchers and that methodological aspects should be based on a normative theoretical framework which explicates the relationship between ethics and technology design.[235] The integration of ethics in the daily work of researchers and developers could be especially important and useful in the case of agile design. In case of agile, the development is a flexible and iterative process, whereby requirements and solutions evolve.[236] This means a continuous integration of ethical considerations in the development process is necessary.

A general analysis of the desirability of data sharing platforms is something that would need to be analysed by policy makers and with a broad stakeholder involvement. This is out of scope of the current project and this deliverable. In this deliverable we will look at certain fundamental values and consider in how far they can be translated into requirements for the technical design of KRAKEN, and to make the ethical implication of certain choices visible.

7.2 Fundamental Moral Principles

This section will use the concept of Principlism to assess possible ethical constraints. As a basis the four principles defined by Beauchamp and Childress[237] will be used, namely respect for persons and autonomy, justice, non-maleficence and beneficence. Furthermore, some additional principles namely dignity, responsibility and accountability will be considered.[238]

---

[232] Anton Vedder, 'Applicable Ethical Guidelines', in: Griet Verhenneman et al., 'WITDOM D6.1 – Legal and Ethical Framework and Privacy and Security Principles', 30.6.2015, 7.

[233] Vedder, 49.

[234] Wessel Reijers et al., 'Methods for Practising Ethics in Research and Innovation: A Literature Review, Critical Analysis and Recommendations', *Science and Engineering Ethics* 24, no. 5 (October 2018): 1447, https://doi.org/10.1007/s11948-017-9961-8.

[235] Reijers et al., 1457.

[236] Inga Kroener, David Barnard-Wills, and Julia Muraszkiewicz, 'Agile Ethics: An Iterative and Flexible Approach to Assessing Ethical, Legal and Social Issues in the Agile Development of Crisis Management Information Systems', *Ethics and Information Technology*, 11 February 2019, 2, https://doi.org/10.1007/s10676-019-09501-6 This move towards agile has raised concerns, especially considering Privacy. See Seda Gürses and Joris van Hoboken, 'Privacy After the Agile Turn' in Jules Polonetzky and others (eds), Cambridge Handbook of Consumer Privacy (Cambridge University Press 2017).

[237] TL Beauchamp, JF Childress, *Principles of Biomedical Ethics* (7th edn, Oxford University Press, 2013)

[238] Biasin et al., 'Safecare D3.9 Analysis of Ethics, Privacy, and Confidentiality Constraints', 67 et seq.

KRAKEN will aim to consider fundamental moral principles, however, as it will be a platform it is not possible to foresee with certainty how the platform will be used in the end.[239] Furthermore, it is often only possible to implement certain values or principles via "proxies", which in itself can again give rise to ethical challenges, as will be explained below.

The ethical considerations exemplified below are therefore only a start, and the inclusion of ethical considerations in the development has to be an ongoing process.

The principle of respect for persons and autonomy: Autonomy is considered to include two conditions, Liberty, which means independence from controlling influences, and Agency, which means the capacity for intentional actions.[240]

KRAKEN does not aim to influence users to share their data in ways the user does not intend. A first consideration is that the use of the KRAKEN platform should always be a free decision and not be obliged by any provider. Autonomy is furthermore operationalized via informed consent. As the information for the informed consent will come from the receiving controller, a possible consideration is how at the side of KRAKEN it could be ensured that the information will indeed be correct and understandable for data subjects.

A proxy which will be used to integrate a certain assurance that the user is acting autonomously is the age requirement. KRAKEN will require users to be above 18 and have full legal capacity, in order to try to ensure that the consent they give to data sharing is valid and autonomously taken. This means that for example, even though it would be legal under the GDPR, parents can in principle not share the data of their children. However, this decision has also ethical implications. The most obvious is that also children and people who do not have full legal capacity can and should be able to act autonomously, and this decision will restrict their autonomy in a certain way. However, considering that a good understanding of the information provided is necessary to make an informed choice, for the moment this restriction seems to be a good choice. It would always be possible to later on change it and open the services of KRAKEN, while possibly including restrictions on the types of data or the purposes. Another implication could be that, if the data obtained via KRAKEN is used for research, the data of children or persons who are not legally capable would not be included, which could result in a bias in the research. In principle, this should be possible to be avoided via good research design on the side of the researcher. Another consideration is the fact that when the data provider is an "origin controller", the data which has legally been obtained could in theory be from e.g. children or legally incapable people, whose parents or guardians have given consent to the processing of the data and for them to be "sold" via KRAKEN, and this might not always be recognizable for KRAKEN. This is an aspect which will be further discussed during the development of KRAKEN. A final consideration with regard to autonomy is the risk of de-anonymisation of anonymized data. As research has shown that it is difficult to properly and securely anonymise data, it might be useful to consider how the data controller might be held responsible for managing anonymized data to prevent re-identification of the data.[241]

The principle of dignity: In the words of Wright dignity "refers to the status of human beings that entitles them to respect and which has to be taken for granted"[242] In the report of the EDPS Ethics Advisory Group it is considered as the basic principle of personhood.[243] A potential risk with regard to

[239] Mark de Reuver et al., 'Digital Platforms and Responsible Innovation: Expanding Value Sensitive Design to Overcome Ontological Uncertainty', *Ethics and Information Technology*, 13 May 2020, https://doi.org/10.1007/s10676-020-09537-z.

[240] David Wright and Emilio Mordini, 'Privacy and Ethical Impact Assessment', in *Privacy Impact Assessment*, ed. David Wright and Paul De Hert (Dordrecht: Springer Netherlands, 2012), 407, https://doi.org/10.1007/978-94-007-2543-0_19.

[241] Biasin et al., 'Safecare D3.9 Analysis of Ethics, Privacy, and Confidentiality Constraints', 69.

[242] Wright and Mordini, 'Privacy and Ethical Impact Assessment', 407.

[243] J. Peter Burgess et al., 'EDPS Ethics Advisory Group Report 2018 - Towards a Digital Ethics', 2018, 30.

'selling' data, which is also recognized by this Group, is that it can lead to data commodification and commoditisation.[244] Commodification is the process where something which was originally not traded becomes an object with economic value and will be traded, while commoditisation is the process whereby customers consider an object of trade as an undifferentiated good.[245] It would be against human dignity if persons would only be considered as 'a source of data'. Another aspect, also related to autonomy, is that it would need to be ensured that not economic necessity would force people to provide their data in order to obtain some money.

The principle of justice: The principle of justice relates to "what is due or owed to a person based on morally relevant properties or situations"[246]. With regard to KRAKEN, some considerations with regard to justice could be whether people could be discriminated based on their data, or whether people might not get access to use KRAKEN or not be paid the proper amount for their data due to e.g. socio-economic status or ethnic origin. One consideration how this can partially be addressed within KRAKEN is that the selection of metadata describing the information in the 'catalogue' should not include any data which could give rise to discrimination.

Ethics-1	The metadata should not provide for discrimination

The principle of non-maleficence: The principle of non-maleficence includes the obligation 'do not harm' but also the obligation to, as far as it is within one's power, not impose risks of harm.[247] Here the questions that should be considered are whether KRAKEN could cause harm or increase the risk of harm? It can for example be considered to ensure the confidentiality, authenticity and integrity of the data.[248]

The principle of beneficence: Going further than the principle of non-maleficence, the principle of beneficence requires to help and contribute to the well-being of others (shortly put: 'maximize possible benefits and minimize possible harms').[249] As with the principle of non-maleficence it should be considered in how far KRAKEN could create harm to people, but additionally also how KRAKEN benefits people and how this benefits can maximised. In particular, the provision and also the analysis of the data should result in an output which evokes potential benefit for the providing data subject, but also for others.[250]

The principle of responsibility: The principle of responsibility requires that a person should fulfil their duties arising from a social or professional role.[251] Due to the interconnectedness of different systems, e.g. in KRAKEN data might be obtained by one system and one (or several) involved actor(s) and then sent via KRAKEN to another (or several) actor(s). Therefore it might be difficult to ascribe responsibility to a single actor.[252] The principle of responsibility also includes that the developers creating KRAKEN act responsibly while developing the system and are respectful of privacy and human rights, which is the aim of KRAKEN from the outset. Responsibility is also important with regard how data should be put to use by different stakeholders and which controls and limitations should apply, which is also in

[244] Burgess et al., 24.
[245] Burgess et al., 24.
[246] E. Biasin, D. Brešić, E. Kamenjašević, P. Notermans, Safecare D3.9 Analysis of ethics, privacy, and confidentiality constraints, 2018, V1, p.67: It is associated with the notions of fairness, desert (in the sense of 'what is deserved') and entitlement, but takes also into account the principle of equality, non-discrimination and property ownership.
[247] Biasin et al., 'Safecare D3.9 Analysis of Ethics, Privacy, and Confidentiality Constraints', 68.
[248] Vedder, p.44.
[249] Biasin et al., 'Safecare D3.9 Analysis of Ethics, Privacy, and Confidentiality Constraints', 68.
[250] Biasin et al., 71.
[251] Biasin et al., 68.
[252] Anton Vedder, 'Applicable Ethical Guidelines', in: Griet Verhenneman et al., 'WITDOM D6.1 – Legal and Ethical Framework and Privacy and Security Principles', 30.6.2015, 44.

particular relevant with regard to the receiving controllers and their use of the data they received.[253] Here it needs to be considered how their responsibility can be ensured, which is partially also via data protection legislation, since, if the data is not anonymous, they will be the controllers of the data and therefore held responsible for the processing of the data.

The principle of accountability: The principle of accountability provides that decisions and actions that are taken should be transparent and that the person responsible can be held accountable.[254] Related to the principle of responsibility, also in this case the implementation of the GDPR requirements can be useful, in particular accountability and transparency provisions. KRAKEN also aims that the data processing will be transparent to users and that users will be able to clearly provide or retract their consent for the data processing.

7.3 Special focus: the monetization of personal data in the EU

Data, including personal data, plays an increasingly critical role in the digital transformation of the EU. In order for the EU to stay competitive and take a leadership role in the digital society, it is necessary to follow a clear approach on the use and governance of data. For these reasons, the European Commission published the 'European strategy for data' on 19 February 2020. With this strategy, the EU aims to create a single market for the free flow of data that makes data more available for use while facilitating the use and monetization of personal data. The European data strategy proposes, among other measures: to adopt legislative measures on data governance, access, and re-use, making data more widely available, and empowering data subjects to stay in control of their data.[255]

KRAKEN, as a privacy-preserving platform that adopts a decentralized user-centric approach, can contribute to the success of the new EU data strategy by offering a privacy-aware marketplace that aims to give control over personal data back to the data subject (*e.g.* SSI management in combination with the dynamic consent management tool). The ability of individuals to make available their data for use (within the limits of their consent) in exchange for rewards aligns with the goal of creating a single market for the free flow of data. As a result, it is important to know whether or not the monetization and transaction of personal data is allowed under the existing EU and national legal frameworks and which limitations may apply.

7.3.1 The monetization of personal data under the EU data protection framework

Under the EU framework, there does not yet exist legislation that explicitly regulates the monetization and transaction of personal data. However, existing legislation applicable to the processing of personal data may provide some initial ideas. In the EU, this subject matter is regulated by the GDPR, which introduces several core data protection principles and obligations for data controllers and processors while broadening the protection of the data subject.

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 or transaction 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

[253] Vedder, 44.
[254] Biasin et al., 'Safecare D3.9 Analysis of Ethics, Privacy, and Confidentiality Constraints', 68.
[255] A European strategy for data, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 19 February 2020, COM(2020) 66 final.

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 (*e.g.* transacting personal data) 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. There are, however, other legal frameworks that regulate specific types of information (*e.g.* rules relating to trade secrets) which may apply.

The GDPR, as a Regulation, applies automatically and uniformly in all Member States. This means that the provisions of the Regulation do not need to be transposed into national law in order for them to be applicable to citizens. This does not mean, however, that the GDPR leaves no room for discretion by the Member States. In fact, several specific provisions in the GDPR allow Member States to introduce more specific rules, restrictions, and limitations (*e.g.* age of consent, legal basis for processing, data subject rights, processing for scientific research purposes, the processing of genetic, biometric, and health data, etc.). Over the past few years, Member States have been adapting their own national data protection frameworks in order to align with the GDPR, as well as introducing additional rules based on Member State discretion (*i.e.* national GDPR implementations). The European Commission has also made clear that Member States, in their implementation, are subject to boundaries:

"*When adapting their national legislation, Member States have to take into account the fact that any national measures which would have the result of creating an obstacle to the direct applicability of the Regulation and of jeopardising its simultaneous and uniform application in the whole of the EU are contrary to the Treaties.*

Repeating the text of regulations in national law is also prohibited (e.g. repeating definitions or the rights of individuals), unless such repetitions are strictly necessary for the sake of coherence and in order to make national laws comprehensible to those to whom they apply. Reproducing the text of the Regulation word for word in national specification law should be exceptional and justified and cannot be used to add additional conditions or interpretations to the text of the regulation."[256]

The additional legal restrictions stemming from national GDPR implementations have to be taken into account when analyzing the possibility to monetize and transact personal data in the EU. Like the GDPR, these national rules do not specifically make reference to the concept of monetizing personal data, but rather regulate specific types of personal data (*e.g.* genetic, biometric, and health data) or processing in relation to a specific legal basis (*e.g.* what is considered as a 'task carried out in the public interest' under national law?). As an example, it may be the case that a Member State prohibits the processing of genetic data for a specific purpose (*e.g.* for life insurance purposes[257]), or that explicit consent may not be relied on as a legal basis for the processing of certain types of sensitive personal data (*e.g.* racial or ethnic origin, political opinions, and religious or philosophical beliefs may not be processed based on the data subject's explicit consent). These rules will also influence the monetization of personal data since it is merely a processing activity in the form of a personal data transfer between parties.

In order to take these legal restrictions into account in the development and design of the platform (in addition to the GDPR), this deliverable contains a list of national GDPR rules (in section 4.6) that could have an influence on the use of personal data in the KRAKEN project and the possibility to monetize and transact personal data.

[256] Stronger protection, new opportunities – Commission guidance on the direct application of the General Data Protection Regulation as of 25 May 2018, Communication from the Commission to the European Parliament and Council, 24 January 2018, COM(2018) 43 final, 9.

[257] E.g. Croatia and Cyprus impose additional restrictions, Greece prohibits the processing of genetic data for health and life insurance purposes.

8 Specific requirements per subsystem

This chapter gives a first indication of which of the identified requirements in this deliverable could potentially be addressed by the different technical teams. This is only a first step and still needs to be further developed during the course of the project.

8.1 Marketplace requirements

One of the first requirements to be considered is DP-2, which is to identify who is controller and who is processor, since it influences the applicability of various other DP requirements. As it is a factual assessment, it might change over time who is considered controller or processor, nevertheless, for the moment the following assumption is made:

For **account/transaction data**: KRAKEN is controller.

For **content data**: KRAKEN is processor, data buyer (receiving controller) is controller & possibly data seller (if it's not a data subject) can also be controller.

8.1.1 For account/transaction data (KRAKEN as controller):

The Table 8 Controller requirements Marketplace below gives an overview of potential requirements for the processing of account and transaction data where KRAKEN is most likely a controller. The requirements are derived from the identified requirements in the previous sections and constitute requirements which can possibly be implemented partially or fully by technical means, or which are organisational requirements which are particularly important. This is only a first step and still needs to be further developed during the course of the project.

Requirement	**Description of the requirement**	
Information/comments		**Potential implementation place**
DP-1:	Identify the type of data which will be processed	
Action: Provide list of data necessary for account creation & transactions		UI
DP-3:	Identify the purpose of the data processing	
Purpose: To be able to provide the KRAKEN service		UI
DP- 4:	Identify the legal ground of processing	
Legal ground: contract with the data subject		UI
DP- 5:	Keep written records of processing activities	
Transaction data: the blockchain will store permanent, unalterable records. *Account data: the SSI and registration modules should provide correspondent log files*		TBD
DP- 5.1.:	Be able to make the written record available to the supervisory authority on request	
Both the blockchain ledger and the log files (See above) can be made easily accessible		N/A
DP- 6:	Facilitate the exercise of data subject rights	

6.1.:	Establish measures to easily retrieve information in the case an access request or an audit is filed
Be able to: • *inform the data subject whether or not personal data concerning him or her are processed* • *provide a copy of the personal data (usually in electronic form) → also: in a structured, commonly used and machine-readable format (to be able to comply with the right to data transfer)* • *provide information*	TBD
DP-6.2.:	Be able to stop the processing of personal data when a data subject request requires it
This will be an extension to user apps and the blockchain back-end, to be developed.	TBD
DP-6.3.:	Be able to rectify the data without undue delay
This should be default functionalities for the marketplace registration workflow	TBD
DP-6.5.:	Be able to erase the data without undue delay
Marketplace accounts should be made easy to erase upon request by the user with no human intervention on our side	TBD
DP- 8:	Provide **information** to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language and in writing.
Consent UI	UI
DP-9:	Implement appropriate technical and organisational measures which are designed to implement data-protection principles in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects; E.g. pseudonymisation, PET
Shared requirement marketplace, crypto, SSI	UI
DP- 10:	Implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed
e.g. Selection of data for consent should by default be not selected, always most data protection friendly possibility selected (user may change it) etc.	UI
DP- 11:	Be able to detect a data breach
	?
DP- 14:	Establish technical and organizational security measures to deploy in the processing and storage of information
Shared requirement marketplace, crypto, SSI *See Annex I for inspiration*	TBD
DP-16:	Only transfer personal data to a third country or an international organization if one of the conditions is given and therefore the level of protection guaranteed by the GDPR is not undermined: • transfer is on the basis of an adequacy decision • transfer is subject to appropriate safeguards • transfer is based on biding corporate rules • one of the derogations of art. 49 is applicable
Still need to be clarified: will any transaction/account data be transferred outside of the EU?	UI?

Ethics-1	The metadata should not provide for discrimination	
The metadata to indicate the data set in the catalogue should be neutral		
ECOM- 1	Establish whether the user is acting as a consumer or a business user	
Relevant to decide which provisions are applicable		UI
ECOM- 2	Include easily reachable at least the following information on the UI (e.g. website) • the name of the service provider • the geographic address at which the service provider is established • details of the service provider, including e-mail address • in case of registration in a trade or similar public register: the register and registration number • in case of VAT: tax registration number	
Art. 5 e-Commerce Directive		UI
ECOM- 3	For the conclusion of a contract with a consumer: provide the following information clearly, comprehensively and unambiguously and prior to the conclusion of the contract: • The different technical steps to follow to conclude the contract; • Whether or not the concluded contract will be filed by the service provider and whether it will be accessible; • The technical means for identifying and correcting input errors prior to the placing of the order; • The languages offered for the conclusion of the contract	
Art. 10 (1) e-Commerce Directive		UI

Table 8 Controller requirements Marketplace

Potentially relevant purely organisational requirements: the following requirements have been added for information purposes, as it still needs to be further discussed whether there could be any technical implementation actions related to them.

DP-12: DPIA

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

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

8.1.2 For content data (KRAKEN as processor):

This Table 9 Processor requirements Marketplace gives an overview of potential requirements for the processing of content data where KRAKEN is most likely a processor, and when content data is personal data or a special category of personal data. The requirements are derived from the identified requirements in the previous sections and constitute requirements which can possibly be implemented partially or fully by technical means, or which are organisational requirements which are

particularly important. These have been selected after discussions with the POs of the scrum teams and the description includes some first considerations, however, this is only a first step and still needs to be further developed during the course of the project.

Requirement	**Description of the requirement**	
Information/comments		**Potential implementation place**
DP-2.1:	establish controller processor agreement in writing with the receiving controller	
Part of the registration process for the data buyer		UI
DP- 3:	Identify the purpose of the data processing	
Individually per receiving controller *Plan is that the data subject can indicate for which purposes it would be willing to provide data* *Possibility for the receiving controller to indicate the intended purpose in the consent form when the data will be bought*?		UI
DP-3.1:	IF data is processed for another purpose AND not based on consent or legislation, controller must make an assessment on whether the processing is compatible with the purpose for which the personal data are initially collected.	
Only indirectly relevant for KRAKEN, mainly relevant for data provider if it is a controller and the data is re-used → should KRAKEN include in the registration a checkbox that if the data is re-used that the controller has made the assessment?		N/A
DP-4:	Identify the legal ground of processing	
Every receiving controller will need to specify the legal ground for processing *Will normally be consent (using the consent interface)*		UI
DP- 4.1.:	IF the processing is based on **consent:** the controller must be able to demonstrate that the data subject has consented to processing of his or her personal data	
DP-4.1.1.:	Consent must comply with the requirements of the GDPR	
DP-4.1.2.:	Include possibility to check that the person consenting is over the age of 18	
Implementation in the consent tool		UI
DP-4.3.:	IF special categories of personal data are processed: explicit consent needed	
Special categories of personal data: personal data which reveal or are: racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, data concerning a natural person's sex life or sexual orientation. *If for example the heart rate is measured and shared, explicit consent is needed* *Implementation in the consent tool* *Related to Requirement 1 → consideration to have different consent for different types of data or simply always request explicit consent*		UI

DP-6:	Facilitate the exercise of data subject rights	
In principle controller obligation, UI include possibility to contact controller		UI
DP-8:	Provide **information** to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language and in writing.	
Consent UI, information must be provided by receiving controller (data buyer)		UI
DP-9:	Implement appropriate technical and organisational measures which are designed to implement data-protection principles in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects; E.g pseudonymisation, PET	
Shared requirement marketplace, crypto, SSI		
DP-10:	Implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed	
e.g. Selection of data for consent should by default be not selected, always most data protection friendly possibility selected (user may change it) etc.		UI
DP- 12:	In case the processing is likely to result in a high risk to the rights and freedoms of natural persons: make a DPIA before the processing. If the result of the DPIA indicates a high risk: consult the supervisory authority	
Not per se required as KRAKEN will not be controller of content data. Request confirmation from receiving controller that the processing will not likely result in a high risk or that a DPIA has been made?		N/A
DP-14:	Establish technical and organizational security measures to deploy in the processing and storage of information	
Shared requirement marketplace, crypto, SSI *See Annex I for inspiration*		N/A
DP- 16:	Only transfer personal data to a third country or an international organization if one of the conditions is given and therefore the level of protection guaranteed by the GDPR is not undermined: • transfer is on the basis of an adequacy decision • transfer is subject to appropriate safeguards • transfer is based on biding corporate rules • one of the derogations of art. 49 is applicable	
To be clarified: receiving controllers outside of the EU? *In that case need to include certain information in the information provision for the data subject and maybe need explicit consent to transfer the data*		UI
DP-17:	Provide sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.	

'catch all clause' – should be automatically fulfilled if the other requirements are fulfilled		N/A
DP-20:	Only process data upon instructions of the controller (except required to do so by Union or Member State law)	
DP- 21:	Keep a written record of all categories of processing activities	
ECOM- 5	Transfer of content data: KRAKEN should not initiate the transmission, select the receiver of the transmission or select or modify the information contained in the transmission	
To avoid liability, Art. 12 e-Commerce Directive ('mere conduit')		TBD
ECOM- 6	Content data: KRAKEN should not monitor the data.	
Upon obtaining knowledge or awareness of illegal activity or information must act expeditiously to remover or to disable access to the information		TBD

Table 9 Processor requirements Marketplace

Potentially relevant purely organisational requirements: the following requirements have been added for information purposes, as it still needs to be further discussed whether there could be any technical implementation actions related to them.

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

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

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

8.2 Crypto subsystem requirements

This table gives an overview of potential requirements for the crypto subsystem. The requirements are derived from the identified requirements in the previous sections and constitute requirements which can possibly be implemented partially or fully by technical means. These have been selected after discussions with the POs of the scrum teams and the description includes some first considerations, however, this is only a first step and still needs to be further developed during the course of the project.

Requirement	**Description of the requirement**	
Information/comments		**Potential implementation place**
DP-14	Establish technical and organizational security measures to deploy in the processing and storage of information	

Shared requirement marketplace, crypto, SSI *See Annex I for inspiration*	

Table 10 Crypto requirements

8.3 SSI subsystem requirements

This table gives an overview of potential requirements for the SSI subsystem. The requirements are derived from the identified requirements in the previous sections and constitute requirements which can possibly be implemented partially or fully by technical means. These have been selected after discussions with the POs of the scrum teams and the description includes some first considerations, however, this is only a first step and still needs to be further developed during the course of the project.

Requirement	**Description of the requirement**	
Information/comments		**Potential implementation place**
DP-9:	Implement appropriate technical and organisational measures which are designed to implement data-protection principles in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects; E.g. pseudonymisation, PET	
Shared requirement marketplace, crypto, SSI		
DP-14:	Establish technical and organizational security measures to deploy in the processing and storage of information	
Shared requirement marketplace, crypto, SSI *See Annex I for inspiration*		
DP-6:	Facilitate the exercise of data subject rights	
DP-6.1.:	Establish measures to easily retrieve information in the case an access request or an audit is filed	
maybe not relevant for SSI?		TBD
DP-6.2.:	Be able to stop the processing of personal data when a data subject request requires it	
This will be an extension to user apps and the blockchain back-end, to be developed.		Blockchain backend
DP-6.3.:	Be able to rectify the data without undue delay	
This should be default functionalities for the marketplace registration workflow, not sure about SSI (probably more complicated)		TBD
DP-6.5.:	Be able to erase the data without undue delay	
Not sure if the SSI has this capability.		TBD

Table 11 SSI requirements

9 Conclusion

This deliverable gave an overview on different requirements and aspects that need to be taken into account during the development of the KRAKEN system. The explication of these requirements is only a first step, and the implementation of these requirements has to follow during the project time. The agile approach which KRAKEN uses demands that the requirements will be included in ongoing development work. A first step has been made by the interaction with the Product Owners of the three main scrum teams and a first selection of possibly relevant GDPR requirements for the scrum teams. Many requirements are more organisational than technical and will therefore depend on the organisational approach which KRAKEN would take in a real-life implementation. Nevertheless, requirements and considerations which can be approached during the technical development will be as far as possible implemented in the KRAKEN system by a close collaboration of the different partners of the project.

10 Bibliography

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', 4 October 2017.

———. 'Opinion 4/2007 on the Concept of Personal Data', 20.6.2007.

Biasin, Elisabetta, Daniela Brešić, Erik Kamenjašević, and Pierre Notermans. 'Safecare D3.9 Analysis of Ethics, Privacy, and Confidentiality Constraints', 2018.

Burgess, J. Peter, Luciano Floridi, Aurélie Pols, and Jeroen van den Hoven. 'EDPS Ethics Advisory Group Report 2018 - Towards a Digital Ethics', 2018.

Campbell, I L. 'Positive Obligations under the ECHR: Deprivation of Liberty by Private Actors'. *Edinburgh Law Review* 10 (2006): 399–412.

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

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 (n.d.).

'Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures'. OJ L 13/12, 19.1.2000.

Domingo, Ignacio Alamillo. 'SSI EIDAS Legal Report - How EIDAS Can Legally Support Digital Identity and Trustworthy DLT-Based Transactions in the Digital Single Market', April 2020.

'ETSI EN 319 411-1 V1.2.2 (2018-04) ETSI EN 319 411-1 V1.2.2 (2018-04)Electronic Signatures and Infrastructures (ESI);Policy and Security Requirements for Trust Service Providers Issuing Certificates;Part 1: General Requirements', n.d.

'ETSI EN 319 412-2 V2.1.1 (2016-02) Electronic Signatures and Infrastructures (ESI);Certificate Profiles; Part 2: Certificate Profile for Certificates Issued to Natural Persons', n.d.

European Data Protection Board. 'Guidelines 4/2019 on Article 25 Data Protection by Design and by Default', 13.11.2019.

———. 'Guidelines 05/2020 on Consent under Regulation 2016/679', 4 May 2020.

———. 'Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR', 2.9.2020.

Felix Bieker, Marit Hansen, and Michael Friedewald. 'Die Grundrechtskonforme Ausgestaltung Der Datenschutz-Folgeabschätzung Nach Der Neuen Europäischen Datenschutz-Grundverordnung', Zeitschrift für Datenschutz-, Informations- und Kommunikationsrecht, no. 4 (2016): 188–97.

Felix Bieker, Michael Friedewald, Marit Hansen, Hannah Obersteller, and Martin Rost. 'A Process for Data Protection Impact Assessment Under the European General Data Protection Regulation'. In *Privacy Technologies and Policy*, 9857:21–37. Lecture Notes in Computer Science. Cham: Springer International Publishing, 2016. http://link.springer.com/10.1007/978-3-319-44760-5.

Graux, Hans. 'STORK 2.0 D3.1 Legal Needs Analysis Report', 8.5.2013.

Kroener, Inga, David Barnard-Wills, and Julia Muraszkiewicz. 'Agile Ethics: An Iterative and Flexible Approach to Assessing Ethical, Legal and Social Issues in the Agile Development of Crisis Management Information Systems'. *Ethics and Information Technology*, 11 February 2019. https://doi.org/10.1007/s10676-019-09501-6.

Laan, V I, and A Rutjes. 'Privacy-issues bij blockchain: hoe voorkom of minimaliseer je die?' *Computerrecht* 2017, no. 6 (17.10.2017): 10.

Patrick Breyer v Bundesrepublik Deutschland, No. ECLI:EU:C:20116:779 / C-258/14 (19.10.2016).

'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'. OJ L 257/73, 28.8.2014.

Reijers, Wessel, David Wright, Philip Brey, Karsten Weber, Rowena Rodrigues, Declan O'Sullivan, and Bert Gordijn. 'Methods for Practising Ethics in Research and Innovation: A Literature Review, Critical Analysis and Recommendations'. *Science and Engineering Ethics* 24, no. 5 (October 2018): 1437–81. https://doi.org/10.1007/s11948-017-9961-8.

Reuver, Mark de, Aimee van Wynsberghe, Marijn Janssen, and Ibo van de Poel. 'Digital Platforms and Responsible Innovation: Expanding Value Sensitive Design to Overcome Ontological Uncertainty'. *Ethics and Information Technology*, 13 May 2020. https://doi.org/10.1007/s10676-020-09537-z.

Verhenneman, Griet, Anton Vedder, Alberto Crespo, Liza Catanzaro, and Francesco Alberti. 'WITDOM D6.1 – Legal and Ethical Framework and Privacy and Security Principles', 30.6.2015.

Vested-Hansen, J. 'Respect for Private and Family Life (Private Life, Home and Communications)'. In *The EU Charter of Fundamental Rights: A Commentary*, edited by S. Peers, T. Hervey, J. Kenner, and A. Ward, 153–82. London: Hart Publishing, 2014.

Wright, David, and Emilio Mordini. 'Privacy and Ethical Impact Assessment'. In *Privacy Impact Assessment*, edited by David Wright and Paul De Hert, 397–418. Dordrecht: Springer Netherlands, 2012. https://doi.org/10.1007/978-94-007-2543-0_19.

Annex I

Measures to be considered during the DPIA (list of measures from the SDM[258]):

Availability[259]:

- Creation of backups of data, process states, configurations, data structures, transaction histories, etc. according to a tested concept
- Protection against external influences (malware, sabotage, force majeure)
- Documentation of data syntax
- Redundancy of hardware, software and infrastructure
- Implementation of repair strategies and backup processes
- Preparation of a contingency plan for restoring processing activity
- Representation arrangements for absent employees

Integrity[260]:

- Restriction of write and modification permissions
- Use of checksums, electronic seals and signatures in accordance with a cryptographic concept
- documented assignment of authorisations and roles
- erasure or rectifying of incorrect data
- Hardening of IT systems so that they have no or as few secondary functionalities as
- possible
- Processes for maintaining the timeliness of data
- Processes for identification and authentication of persons and equipment
- Definition of the intended behaviour of processes and regular tests to determine and document functionality, risks, security gaps and side effects of processes
- Determination of the target behaviour of processes and procedures and regular performance of tests to ascertain or determine the current state of processes
- Protection against external influences (espionage, hacking)

Confidentiality[261]:

- Definition of an authorisation and role concept according to the necessity principle on the basis of identity management by the controller
- Implementation of a secure authentication procedure
- Limitation of authorised personnel to those who are verifiably responsible (locally, professionally), qualified, reliable (if necessary, with security clearance) and formally approved, and with whom no conflict of interests may arise in the exercise of their duties
- Specification and monitoring of the use of authorised resources, in particular communication channels
- specified environments (buildings, rooms) equipped for processing activities

[258] Conference of the Independent Data Protection Supervisory Authorities of the Federation and the Länder, 'The Standard Data Protection Model', 31 et seqq.
[259] Conference of the Independent Data Protection Supervisory Authorities of the Federation and the Länder, 31.
[260] Conference of the Independent Data Protection Supervisory Authorities of the Federation and the Länder, 32.
[261] Conference of the Independent Data Protection Supervisory Authorities of the Federation and the Länder, 32.

- Definition and monitoring of organisational processes, internal regulations and contractual obligations (obligation to maintain data secrecy, confidentiality agreements, etc.)
- Encryption of stored or transferred data and processes for managing and protecting cryptographic information (cryptographic concept)
- Protection against external influences (espionage, hacking).

Unlinkability[262]:

- Restriction of processing, use and transfer permissions
- Program-wise omission or deactivation of interfaces in processing methods and components
- Regulatory measures to prohibit backdoors and quality assurance audits for compliance in software development
- Separation according to organisational/departmental boundaries
- Separation by means of role concepts with graduated access rights on the basis of identity management by the controller and a secure authentication process
- Approval of user-controlled identity management by the controller
- Use of purpose specific pseudonyms, anonymisation services, anonymous credentials, processing of pseudonymous or anonymised data
- Regulated processes for amending the purposes of the processing

Transparency[263]:

- Documentation in the sense of an inventory of all processing activities in accordance with Art. 30 GDPR
- Documentation of the components of processing activities, in particular business processes, databases, data flows and network plans, IT systems used for this purpose, operating procedures, descriptions of processing activities, interaction with other processing activities
- Documentation of tests, of the release and, where appropriate, the data protection impact assessment of new or modified processing activities
- Documentation of the factors used for profiling, scoring or semi-automated decisions
- Documentation of contracts with internal employees, contracts with external service providers and third parties from whom data is collected or transmitted, business distribution plans, responsibility regulations
- Documentation of consents, their revocation and objections
- Logging of accesses and changes
- Versioning
- Documentation of processing by means of protocols on the basis of a logging and evaluation concept
- Documentation of the data sources, e. g. the implementation of information duties towards data subjects where their data were collected and the handling of data breaches

[262] Conference of the Independent Data Protection Supervisory Authorities of the Federation and the Länder, 33.
[263] Conference of the Independent Data Protection Supervisory Authorities of the Federation and the Länder, 33–34.

- Notification of data subjects in the event of data breaches or further processing for another purpose
- Traceability of the activities of the controller for granting data subjects' rights
- Consideration of the information rights of data subjects in the logging and evaluation concept
- Provision of information on the processing of personal data to data subjects

Intervenability[264]:

- Measures for differentiated consent, revocation and objection options
- Creation of necessary data fields, e. g. for blocking indicators, notifications, consents, objections, counterstatements
- documented processing of faults, problem handling and changes to processing activities as well as to technical and organisational measures
- Possibility of deactivating individual functionalities without affecting the overall system
- Implementation of standardised query and dialogue interfaces for data subjects to assert and/or enforce claims
- Operation of an interface for structured, machine-readable data for the retrieval by data subjects
- Identification and authentication of persons who wish to exercise data subjects' rights
- Establishment of a Single Point of Contact (SPoC) for data subjects
- operational possibility of compiling, consistently rectifying, blocking and erasure of all data stored on a person
- Provision of options for data subjects in order to be able to set up programs in line with data protection requirements

Data Minimisation[265]:

- Reduction of recorded attributes of data subjects
- Reduction of processing options in each processing step
- Reduction of the possibility of gaining knowledge of existing data
- Establishing default settings for data subjects which limit the processing of their data to what is necessary for the purpose of the processing.
- Preference for automated processes (not decision processes), which make it unnecessary to gain knowledge of processed data and limit influence in comparison to dialogue controlled processes
- Implementation of data masks that suppress data fields, and automatic blocking and erasure routines, pseudonymisation and anonymisation processes
- Definition and implementation of an erasure concept
- Rules for the monitoring of processes to change processing activities

[264] Conference of the Independent Data Protection Supervisory Authorities of the Federation and the Länder, 34–35.
[265] Conference of the Independent Data Protection Supervisory Authorities of the Federation and the Länder, 35.

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