NGI TRUST CHAIN

TrustChain Legal, Regulatory and Ethical Report

30/06/2023

Funded by the European Union

TrustChain Project. Funded by the European Union under GA No 101093274. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the granting authority can be held responsible for them.

Grant Agreement No.: 101093274
Call: HORIZON-CL4-2022-HUMAN-01
Topic: HORIZON-CL4-2022-HUMAN-01-03
Type of action: RIA

D4.6 Legal, Regulatory and Ethical Framework

Guidance for open call participants

Work package	WP 4
Task	T4.2
Due date	30/06/2023
Submission date	30/06/2023
Deliverable lead	Timelex
Version	1.0
Authors	Ruben Roex (Timelex)
Reviewers	Raj Rajarajan (City, University of London) Georgios Stamoulis (Athens University of Economics and Business)
Abstract	This Deliverable provides all open call participants with an overview of the main ethical, legal and regulatory obligations they should take into account when developing their projects.
Keywords	Law, Data Protection, GDPR, Trust Services, eIDAS

Funded by the European Union

Document Revision History

Version	Date	Description of change	List of contributor(s)
1	25/6/2023	First draft	Ruben Roex (Timelex)

DISCLAIMER

COPYRIGHT NOTICE

The TRUSTCHAIN Consortium is the following:

Participant number	Participant organisation name	Short name	Country
1	EUROPEAN DYNAMICS LUXEMBOURG SA	ED	LU
2	F6S NETWORK IRELAND LIMITED	F6S	IE
3	UNIVERZA V LJUBLJANI	UL	SI
4	ATHENS UNIVERSITY OF ECONOMICS AND BUSINESS - RESEARCH CENTER	AUEB	EL
5	FUNDACION CIBERVOLUNTARIOS	CIB	ES
6	CONSORCIO RED ALASTRIA	ALA	ES
7	TIMELEX	TLX	BE
8	CITY UNIVERSITY OF LONDON	ICS	UK

EXECUTIVE SUMMARY

An heterogeneous legal framework

Taking into account the scope of the open calls of project TRUSTCHAIN and the emphasis on human-centricity, it should not come as a surprise that participants to the open calls have a range of ethical and legal concerns they should account for. In this deliverable the main concerns are highlighted and explained. The objective is not to be as comprehensive as possible, but rather to make the sometimes complicated ethical and legal instruments more understandable to readers who do not have legal background.

It would be impossible to map out and explain every single instrument which may be applicable to the participants' projects. Hence, this deliverable focuses on those instruments which can be expected to apply for most of them.

In the first Chapter the ethical aspects are covered, with particular attention to the obligations of the General Data Protection Regulation (GDPR). In a question-and-answer format the key obligations imposed by data protection law are explained.

In the second Chapter, the main legal instruments are covered. The impact of the new cybersecurity framework created by the NIS2 Directive and the upcoming new framework for trust services created by the European Digital Identity Regulation (i.e., ARF) are explained. The chapter ends with a brief overview of other instruments which will have a bearing on many projects, such as digital services, e-commerce, consumer protection and intellectual property.

With the overview provided in this deliverable, the participants should have a first indication of how these different legal instruments may impact their respective projects. Of course, the participants will still be required to specifically apply these instruments to their activities and projects, because this deliverable will not replace tailored legal advice.

TABLE OF CONTENTS

ABBREVIATIONS

EDIR	European Digital Identity Regulation
EDIW	European Digital Identity Wallet
eIDAS	electronic Identification, Authentication and Trust Services
GUI	Graphical User Interface
HER	Horizon Europe Regulation
NIS	Network and Information System
RRI	Responsible Research and Innovation
GDPR	General Data Protection Regulation

1 INTRODUCTION

1.1 CONTEXT

The overall objective of TrustChain is to create a portfolio of Next Generation Internet protocols and an ecosystem of decentralised software solutions that reach the highest standards of humanity such as those chartered by the United Nations including the respect of human rights, ethics, sustainability, energy efficiency, our care for the environment and our respect for the World's cultural history. To achieve this objective, five open calls will be organized in a systematic manner to build the necessary building blocks of the next generation decentralised internet. The open calls are intended to identify and select top internet system innovators who can help with the creation of innovative building blocks and sub-systems that can help to create the decentralised next generation internet.

The primacy of ethics and respect for the rule of law are two essential drivers of the TrustChain project, as is abundantly clear from its objective description. To ensure that these two essential drivers are observed throughout TrustChain, all of the selected innovators in the open call process must be made aware of them.

1.2 OBJECTIVE

The objective of this deliverable is to raise awareness of the ethical and legal aspects which are most relevant to TrustChain. It provides the participants to the open call with guidance and handles on how to account for, and implement, the applicable ethical and legal considerations and obligations in their work and solutions. It maps out the statutory instruments at EU level which are most relevant to the open calls and provides practical guidance on the operational application of the obligations contained in these instruments. As such, this first report takes an "as-is" prescriptive perspective. The second legal report will be more forward looking and will consider how the novel solutions developed in TrustChain may challenge the existing legal framework.

The goal of this deliverable is not to be as exhaustive and detailed as possible, since it would be impossible to identify beforehand how the ethical principles and legal instruments should be implemented in every single solution (still to be) developed in the open calls. It rather takes a more overarching perspective and provides pointers on how to account for ethical and legal obligations that can be expected to be common to most, if not all, of the open call solutions. The overarching perspective offered in this deliverable will in any case be complemented by the more tailored guidance offered to the open call participants during the different implementation phases of the open calls. To the extent that cross-cutting questions are identified when interacting with the open call participants directly, these will be added to the second legal report which is due in month 24 of the project (i.e. by the end of 2024).

1.3 APPROACH

This deliverable providing guidance on the ethical, regulatory and legal issues relevant to TrustChain is not the only deliverable meant to assist the Open Call participants in developing and implementing their solutions in accordance with the TrustChain objectives. There are other deliverables which have the same objective but take a somewhat different angle (e.g., D3.4 Guide for Open Call implementation and D4.1 Methodological guidelines for the Open Calls user-centred approach). Whereas D3.4 provides a succinct overview of technical, user-centric and ethical and legal aspects to be considered by the open call participants, this deliverable complements the succinct overview with a more detailed, in-depth description of the ethical, regulatory and legal aspects.

Funded by the European Union

The approach followed in this deliverable is the same for every legal instrument considered and discussed. Firstly, a general description of the instrument is given and the main field of application discussed. Secondly, a practical overview of the main obligations/implications is provided with examples where necessary. Thirdly, where relevant the Deliverable includes templates of documents which can be used by the open call participants to ensure compliance with their legal obligations.

Disclaimer: Any templates provided herein are meant for informational purposes only and will require adaption by the open call participants to their own circumstances. The templates should not be used "as-is" in the participants' specific setting.

2 ETHICAL CONSIDERATIONS

2.1 INTRODUCTION

In this section the most relevant ethical considerations in relation to TrustChain are discussed. While ethical considerations are quite often tied with regulatory and legal obligations, in the sense that the law is meant to protect key ethical and moral considerations and values, they are nonetheless of a different nature. Whereas regulatory and legal obligations are explicitly set forth in law, ethical considerations do not have such explicit basis. Nonetheless, Article 19 of Regulation (EU) 2021/695 on Horizon Europe (hereinafter: the "HER") makes compliance with ethical principles mandatory. That provision refers to the mandatory completion of an ethical self-assessment and compliance with the European Code of Conduct for Research Integrity as key requirements to ensure ethical conduct during Horizon Europe-funded actions such as TrustChain.

2.2 RELEVANT ETHICAL DOMAINS

While the HER lists several ethical domains which are to be particularly considered (see Art. 19.1 HER), only a few of these seem relevant to TrustChain. These are (a) the right to privacy and data protection and (b) the right to equality (which is of particular relevance considering the user-centric approach). The ethical self-assessment furthermore refers to (c) the involvement of humans in the action, which, again, is the case in TrustChain due to the user-centric approach. However, the risks associated with human involvement in the action mainly relates to the two aforementioned main ethical domains, i.e. data protection and equality. Considering the relevance of these domains, they will be considered in more detail below.

2.3 PRIVACY AND PERSONAL DATA PROTECTION

2.3.1 Introduction

The protection of the right to privacy and the right to data protection are not only ethical considerations, but are rights which are enshrined in the Charter of Fundamental Rights of the European Union (hereinafter: "the Charter"). Article 7 of the Charter sets forth the right to privacy (i.e. the right to respect for private and family life, home and communications), whereas Article 8 sets forth the protection of personal data. Where the right to privacy has been included in many constitutions and has been the subject of case law at the national, supranational and international level, it is arguably the protection of personal data that recently has gained the most attention and which is the most relevant to consider in TrustChain.

Whilst having the status of fundamental right, the right to the protection of personal data has been further elaborated on and specified by the European legislator in a number of regulations and directives.

The most relevant of those for TrustChain would be Regulation (EU) 2016/679 (i.e. the General Data Protection Regulation or GDPR).

2.3.2 Field of application of the GDPR

Article 2 GDPR clarifies that the GDPR applies among others to anyone who processes personal data using any sort of digital device ("automated means"). Hence, irrespective of whether an open call participant is a natural or legal person, or whether that participant is a private or public sector entity, as soon as personal data are processed as part of the proposed solution, the GDPR will automatically apply.

Considering that the objective is to protect a fundamental right, concepts in the GDPR are typically interpreted broadly. Similarly, the concept of "personal data" as defined in Art. 4.1 GDPR should be interpreted broadly. Any information which can potentially be linked to a natural person, irrespective of whether that person is known by name or identifiable through some other type of identifier (an IP address, a number or other unique parameter), should be considered to be personal data. Most, if not all, of the proposed solutions in the open call will involve the processing of personal data and should thus comply with the requirements of the GDPR.

Considering that the GDPR itself is quite an extensive instrument and case law in the domain is rapidly developing and evolving, it would be overly ambitious to try and cover all of the GDPR's obligations and requirements in this deliverable. Hence, to keep things practical for open call participants, this section will touch upon the GDPR's key requirements in the form of a questionnaire with explanations. This should help each participant to identify which actions are to be taken to ensure compliance with the GDPR and therefore respecting the ethical considerations related to privacy and data protection.

2.3.3 Key requirements in relation to personal data processing

2.3.3.1 Personal data and data subjects

Question 1:	What type of personal data will the participant be collecting when developing and/or implementing the solution in TrustChain and to what category(-ies) of individuals (called "data subjects") do they relate?
Explanation:	While all types of personal data are protected under the GDPR, there are certain categories of personal data which raise particular concerns and which are in principle prohibited from being processed. The categories of personal data which raise special concerns are (Art. 9.1 and 10 GDPR): data revealing 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 or data concerning a natural person's sex life or sexual orientation and personal data related to criminal convictions and offences or related security measures. If the participant's solution processes any of the aforementioned categories of personal data, the participant should carefully read through Art. 9.2 GDPR and any relevant guidance offered by competent authorities to ascertain whether the participant is allowed to process these data. If the participant remains unsure, the participant should consult its organization's data protection officer or an independent expert. While the GDPR requires personal data of any natural person to be protected, irrespective of personal characteristics, nationality or location, certain categories of vulnerable individuals require extra attention. This is the case for children (e.g. Art. 8 GDPR), patients (e.g. Art. 9.2 GDPR), employees (e.g. Art. 88 GDPR), etc. When these

	categories of individuals are involved, the participant should pay extra attention whether any specific needs need to be accommodated, such as involvement of a legal guardian, increased information obligations, additional safeguards for the data processed, etc.

2.3.3.2 Reasons for processing and legal basis

Question 2:	For which purposes will the participant be collecting and using the personal data?
Explanation:	The participant must explicitly identify and delineate the purposes for which the personal data will be collected and used. There is no limit to the number of purposes which can be identified, but any purpose for which the participant wants to use the personal data must be explicitly delineated. All purposes must be mentioned in an information notice addressed to the data subjects. The purposes must be legitimate. The identified and notified purposes will in part help determine which legal basis is appropriate for processing the personal data. For instance, if the data are collected because the law requires it, the purpose will be determined by law and the legal basis for processing will be the necessity to comply with a legal obligation to which the participant is a subject.

Question 3:	Will the participant collect and use the personal data by asking the data subjects for their consent, are the personal data necessary to perform a contract with the data subjects or will the participant invoke another legal basis?
Explanation:	The GDPR requires that each personal data processing activity has a legal basis. In practice this means that the participant must assess what the purposes are for processing personal data (see previous question) and should then consider which of the six legal bases listed in Article 6.1 GDPR can be used to legitimize the processing activity. These six legal bases are: 1. Consent of the concerned individual (a template consent form has been added in Appendix A of this deliverable) (Art. 6.1.a GDPR). 2. Necessity of the processing for the performance of a contract between the participant and the concerned individual (the processing must truly be necessary for the conclusion, performance or termination of an agreement between the participant and the concerned individual. A contract with another third party does not count) (Art. 6.1.b GDPR). 3. Necessity of the processing to comply with a legal obligation (Art. 6.1.c GDPR). 4. Necessity of the processing to protect the vital interest of the concerned individual or of someone else (it does not seem likely that this will apply in the context of TrustChain open calls) (Art. 6.1.d GDPR). 5. Necessity of the processing to perform a task in the public interest (Art. 6.1.e GDPR). 6. Necessity of the processing for the purposes of the legitimate interests of the participant or a third party (Art. 6.1.f GDPR). It should be noted that when people are asked to participate in an experiment and their personal data is collected as part of the experiment, it is customary to ask for

consent but it is still warranted to check whether other legal bases can apply. Consent can always be withdrawn, which should always be borne in mind.

2.3.3.3 Quality requirements of every processing activity

Question 4:	How will the participant ensure that? a) the data subjects are appropriately informed and nothing is processed without proper information having been provided? b) the personal data are only used for the communicated purposes? c) no personal data is collected beyond the data truly required to achieve the purposes? d) the personal data are accurate and up to date? e) the personal data are de-identified when no longer necessary for the communicated purposes? f) the personal data are kept safe and confidential?
Explanation:	Article 5 GDPR requires every processing activity to adhere to certain quality requirements. For each of the 6 sub-questions listed above the participant should assess how each question can be adequately answered to ascertain that all quality requirements are met. It starts of course with a good understanding of what the participant is trying to achieve and how best to achieve it. This understanding should then be communicated in an appropriate manner to the concerned individual, personal data should never be processed secretively.

2.3.3.4 Providing information

Question 5:	How can the participant adequately inform the data subjects?
Explanation:	First of all, it should be noted that data subjects must in principle be informed *before* any processing activity takes place. If personal data are not received from the data subjects themselves but from another source, the participant has one month to inform the data subjects unless the data are used to communicate with the data subjects. In the latter case, the data subjects must be informed at the point of first communication. It is the participant's burden to demonstrate that the data subjects have been informed! Secondly, the information provided to the data subjects must be comprehensible, concise and accurate and should ideally be provided in writing (either through digital means or on paper). This means that it should be written in a language that the data subjects understand (note that not everyone understands English!), that it should not use overly complicated legal language, be excessive in length (e.g. by including a lot of information which is not relevant) or be ill-suited or outdated in relation to the processing envisaged in TrustChain. Thirdly, the contents of the information notice are largely determined in Articles 13 and 14 GDPR, which means that the participant cannot freely choose the information it wants to provide.

2.3.3.5 Data subject rights

Question 6:	Which rights can data subjects exercise against participants?
Explanation:	Chapter III GDPR outlines the different rights which data subjects have in relation to the participant processing their personal data. Apart from the right to information, which has already been outlined above, there are 7 rights in total which data subjects can exercise vis-à-vis the participant acting as controller. These rights include: 1. The right of access (and copy) (Article 15 GDPR); 2. The right to rectification (Article 16 GDPR); 3. The right to erasure (Article 17 GDPR); 4. The right to restriction (Article 18 GDPR); 5. The right to data portability (Article 20 GDPR); 6. The right to object (Article 21 GDPR); 7. The right not to be subject to automated decision-making (Article 22 GDPR). The right to access provides the data subjects upon their request with detailed information about the personal data which the participant processes about them as well as a copy of that data in a human-readable format. The right to rectification provides data subjects with the right to request that personal data which is erroneous, is corrected. The right to erasure provides data subjects in a limited set of circumstances with the right to request that personal data about them is erased. This does not mean that the data subjects can always ask for erasure, but only in those circumstances where Article 17 GDPR explicitly allows it. The right to restriction allows data subjects to request that their personal data are only processed for one of the four purposes listed in Article 18 GDPR. They can no longer be processed for other purposes, which typically means extracting the data from operational systems and storing them somewhere separately to avoid that they are used for other purposes. The right to data portability allows data subjects to request a machine-readable copy of the personal data which they themselves have provided to the participant in an electronic format, so that these personal data can then be easily uploaded in a competing system. The right to object allows data subjects to oppose the processing of personal data when such processing is based on the necessity of the processing for the purposes of the legitimate interests of the participant or a third party. The right not to be subject to automated decision-making, including profiling, entails data subjects' right to demand that decisions about them are not solely based on automated processing, including profiling. Put differently, they can ask for a human review. A controller must be able to comply with these rights, irrespective of the technologies used. In highly distributed environments like blockchains, it may not be easy to comply with them. Please note that the GDPR does not foresee exceptions to data subject rights for reasons of technical complexity, it only allows for exceptions in case the controller is no longer able to identify the data subject (Article 11 GDPR).

2.3.3.6 Relationships with third parties

Question 7:	Will the participant rely on third parties to undertake the whole or part of the processing (e.g. a cloud hosting company which takes care of hosting the personal data)?
Explanation:	Whenever a participant relies on the services of a third party to undertake the whole or a part of the processing of personal data on behalf of the participant, the third party will act as a processor. The third party will not be allowed to use the personal data entrusted to it by the participant for its own purposes, but will only be allowed to process the personal data as instructed by the participant. Article 28 GDPR requires the participant to carefully select its processors. Only those parties which offer sufficient guarantees that they can process the personal data entrusted to them in a safe and secure manner should be chosen. Article 28.3 GDPR also requires participants to conclude a so-called data processing agreement with their third-party service providers. The content of the data processing agreement has largely been determined by law: Article 28.3 GDPR lists which clauses should minimally be included in a data processing agreement. The European Commission has drafted a model contract which any controller can use when contracting with a processor. For participants' convenience, this model contract can be found here: https://commission.europa.eu/publications/standard-contractual-clauses-controllers-and-processors-eueea_en. The benefit of this model contract is that participants no longer need to come up with their own legal language to comply with Article 28.3. They can simply use the model contract, make the necessary choices in the template's main body of text and complete its annexes.

Question 8:	Will the participant make personal data accessible or actively send personal data to a third party (a service provider, affiliate, partner, etc.) which is not based in the European Union?
Explanation:	Chapter V GDPR sets out the conditions and requirements under which a participant is allowed to transfer personal data from within the European Economic Area[1] to one or more recipients in countries outside the European Economic Area.[2] The main requirement is that the level of protection offered to personal data in the recipient country pursuant to a transfer from the European Economic Area should be essentially equivalent to the level of protection offered within the European Union. Such equivalent level of protection can be offered by (a) the legislation and institutional framework in the recipient country itself or (b) arrangements that the data exporter and importer put in place between them to ensure such equivalent protection. If an equivalent level of protection is not possible, personal data could still

[1] The European Economic Area consists of the member states of the European Union, Norway, Iceland and Liechtenstein. The UK is not a part of the European Economic Area.

[2] There are no such conditions for transfers of personal data within the European Economic Area.

be transferred in occasional circumstances where one of the derogations in Article 49 GDPR applies.

In practice, participants must first assess whether they will engage in a transfer to a country which has been given an adequacy decision by the European Commission. The list of countries that has received an adequacy decision can be found here: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en. An adequacy decision essentially means that the country has been whitelisted as offering a level of protection for personal data which is equivalent to the protection offered in the European Economic Area. The participant does not have to do anything additional for the transfer than what has to be done for any other personal data processing activity.

If a recipient country does not appear on the list of countries for which an adequacy decision exists, the participant will most likely have to resort to a contractual mechanism ensuring adequate protection. This contractual mechanism typically takes the form of standard contractual clauses for the transfer of personal data. The standard contractual clauses (often abbreviated as "SCC") are a model contract provided by the European Commission that parties to a data transfer can sign between them to ensure adequate protection of the personal data transferred. The contractual clauses themselves cannot be modified, but must be used "as-is". You can add clauses to them, however, to the extent that these additions do not change the level of protection offered by the existing clauses. The SCC consist of four modules, depending on the qualifications of the parties (controller-to-controller, controller-to-processor, processor-to-processor and processor-to-controller). The parties must select the correct module to apply, complete the annexes and each in turn sign the SCC.

Pursuant to case law of the European Union Court of Justice, it is no longer sufficient to rely on SCC alone. The participant who intends to transfer personal data to a country which does not have an adequacy decision, should perform a transfer impact assessment. This entails an assessment of the recipient country's legal and institutional framework to ascertain whether there are particular risks in the recipient country that governmental entities such as intelligence and police agencies and bodies have broad powers to access the personal data transferred without due protection and redress mechanisms for the data subjects concerned. The European Union Court of Justice found that the US for instance has far too broad powers for its intelligence services without adequate protection and redress mechanisms for non-US data subjects. If the participant nonetheless wants to transfer personal data to a country that does not offer adequate protection, the participant will have to ensure that supplementary measures are taken which prevent foreign authorities gaining access to the transferred personal data. The European Data Protection Board has offered guidance on the supplementary measures that can be taken: https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en.

2.4 ETHICS BEYOND DATA PROTECTION

2.4.1 Methodology for performing an ethics assessment

In contrast with the domain of data protection, where the law already provides clear guidance on how participants can implement ethical concerns related to data protection into their work, a concrete way of working is less clear for the other ethical domains. Hence, participants could, from a methodological perspective, contemplate using the EU's framework for Responsible Research and Innovation.[3] As described by the Commission, RRI implies that societal actors (researchers, citizens, policy makers, business, third sector organisations, etc.) work together during the whole research and innovation process in order to better align both the process and its outcomes with the values, needs and expectations of society.

The objective of the ethics tasks of participants is to ensure that the innovation brought about by their project is in line with European ethics and moral values. This is done by applying the theory of Value Sensitive Design[4], an approach which aims to integrate a wide range of human and moral values into the design of (information) technology.

In other words, Value Sensitive Design implies that a normative framework is defined, and that the designers of a system – in this case the participant – integrates this framework into the participant's work, thus recognising that systems are rarely ethically neutral, and that human well-being, human dignity, justice, welfare, and human rights can be served by integrating them into technological design.

Therefore, as a first step, a usable normative framework must be established for the participant's project, and specific ethics requirements must be derived on the basis of this framework.

2.4.2 Normative framework and ethics requirements

Any ethics evaluation requires an explication of the normative framework against which the anticipated innovation is to be assessed. The Open Call documents as made available by the TrustChain consortium already make it clear that the central ethical concern is compliance with the fundamental right to data protection. Hence, the extensive guidance provided on that topic above. More broadly however, participants should assess the extent to which their project complies with European values as enshrined in the Charter of Fundamental Rights of the European Union – which includes, but is not limited to, the right to data protection and privacy. The remit of ethics and the scope of European values is indeed broader than data protection and privacy alone. The Charter applies a structure of six value domains, each of which warrant specific scrutiny in the participants' projects:

- Dignity, notably individuals' right to be secure in their physical and mental integrity.
- Freedoms, comprising the rights to data protection and privacy, but also intellectual freedoms (education, expression, thought, religion and information) and social freedoms (assembly, marriage, asylum and property);
- Equality, including non-discrimination and rights of minorities and of societally more vulnerable parties;
- Solidarity, covering workers' rights and labour rights, social security, collective bargaining, health care and environmental protection;
- Citizens' rights, such as the right to vote, to proper administration, access to documents and freedom of movement;

[3] https://op.europa.eu/en/publication-detail/-/publication/ee9bacdf-fdad-46eb-8cd8-32879e3101911/language-en.

[4] https://vsdesign.org/publications/.

Funded by the European Union

- Justice, including access to fair trial and effective remedy, and the right to defence.

These values collectively comprise the normative framework to be applied as a yardstick in participants' evaluation of their project. The TRUSTCHAIN project has as its broad objective the promotion of many of the aforementioned values (e.g. by means of applications for digital identities, TRUSTCHAIN will help facilitate citizens in exercising their rights).

The most relevant of the aforementioned values, next to data protection, which may potentially raise concerns, would seem to be *equality*.

A potential risk in a participant's project, may be that the participant's services would be accessible only to parties with adequate digital literacy and adequate digital infrastructure and connectivity, thus becoming a manifestation of the digital divide concern: some parties would benefit from the participant's solution due to their capability of working with a potentially complex IT system, whereas others would be left behind for reasons beyond their reasonable control. This would be particularly detrimental in the context of TrustChain, since the goal is to build inclusive, human-centred solutions.

This concern should always be mitigated in the context of the participants' projects because they are required to follow a human-centric approach: users in use cases can be selected to ensure that accessibility is not an issue. Accessibility of the design – in terms of technical user friendliness and complexity, as well as e.g. choice of language and guidance for users – should none the less remain a priority in the project in order to mitigate any inequality concerns. Participants are encouraged to check Trustchain Deliverable 4.1 for more guidance on setting up an appropriate human-centred design approach.

3 LEGAL AND REGULATORY CONSIDERATIONS

In addition to the ethical considerations discussed in the previous chapter, there are quite a few legal and regulatory considerations to be taken into account by the open call participants as well. As mentioned above, it would be virtually impossible to account for every single instrument which may have a bearing on the projects proposed by the participants. Hence, this chapter will provide the participants with an overview of relatively new, and perhaps not yet fully understood, instruments which can be presumed to be relevant to most, if not all, projects. For each instrument the field of application and the main obligations will be described. Please note that this deliverable does not cover topics which are common to every research project and can therefore be presumed to be known to the participants already, such as general contract law.

3.1 NETWORK AND INFORMATION SECURITY

In addition to the GDPR's specific rules for the protection of personal data as described in the previous chapter, the European Union introduced in 2016 a more general framework to strengthen cybersecurity in all Member States. Up until then, cyber security provisions were introduced in an ad hoc fashion in a number of different instruments and were largely left to Member States' own discretion. This led the vast discrepancies between Member States with regard to the overall level of cybersecurity maturity. At the same time, cyber threats continued to grow exponentially in both volume and complexity, leading to significant economic and social damages for everyone who fell victim to these threats.

These developments incentivized the European legislator to introduce in 2016 the Network and Information Security Directive ("NIS Directive"). This instrument forced Member States to at least achieve a minimum level of cybersecurity by adopting a national cybersecurity strategy, putting in place a national governance and oversight structure and imposing minimum security obligations upon a number of service providers which were considered to be critical to society.

Funded by the European Union

In 2020 the European Commission noted that the NIS Directive did not provide a fully satisfactory answer to the rapidly evolving threat landscape and introduced a proposal for an update to the NIS Directive. The second iteration of the NIS Directive, conveniently referred to as the NIS2 Directive (i.e. Directive (EU) 2022/2555), entered into force on 16 January 2023. This new version brings more services and activities within its scope, imposes additional obligations on the providers of those services and activities and introduces a more effective enforcement mechanism.

3.1.1 Field of application

Question 1:	What are these "network and information systems" referred to under the NIS2 Directive?
Explanation:	The definition of "network and information system" in Article 6.2 NIS2 Directive is relatively broad and encompasses networks, devices running software for processing data as well as the data itself. Hence, when considering measures to be taken to protect network and information systems, one should consider all of these three layers.

Question 2:	Are **all** network and information systems in scope of the NIS2 Directive?
Explanation:	No, the NIS2 Directive applies only to network and information systems which are used by essential and important entities for their operation and the provision of their services. Annex I and II list the sectors where essential and important entities are to be found. These sectors include, among others: 1. digital infrastructure, including cloud computing service providers and trust service providers; 2. ICT service management (business-to-business). While the NIS2 Directive excludes certain small and medium-sized enterprises from its scope, the size criterion does not apply to providers of trust services. Simply put, if a participant offers a service governed by the eIDAS Regulation, that service provider will fall under the NIS2 Directive.

Question 3:	Will the rules be the same for every participant across the European Union?
Explanation:	The NIS2 Directive remains, as its predecessor, a directive and not a regulation. Consequently, every Member State will have to transpose the NIS2 Directive's provisions into its national legislation. It is to be expected that there will be deviations between Member States' transpositions. The previous NIS Directive has shown that these deviations can be significant in practice. It is therefore important for each participant to determine which Member State's national cybersecurity law will apply. Please note that the Member States will have until the 17th of October 2024 to transpose the national rules. Nothing prevents Member States from transposing sooner, however, and quite a few Member States have indicated to have started already on updating their national legislation. Participants are therefore encouraged to keep track of relevant national developments.

Question 4:	How does the participant know which Member State's rules to apply?
Explanation:	The territorial application of the NIS2 Directive is largely determined in its Article 26. For cloud computing service providers and providers of managed services, the rules of the Member State where the provider has its main establishment will apply. For trust service providers it would be the Member State where they are established. Hence, the first test for every participant is to assess which type of service the participant provides. The next step is then determining which Member State's law will apply. In a third step, and dependent on the national transposition, the participant will be able to assess which of its operations and activities using network and information systems are in scope.

3.1.2 Obligations under the NIS2 Directive

The main obligations for participants under the NIS2 Directive are explained in its Articles 21 and 23. Article 21 covers all preventive cybersecurity risk-management measures that the participant should take, whereas Article 23 deals with the obligation to notify incidents and cyber threats.

Question 5:	Which preventive cybersecurity risk-management measures does a participant have to take?
Explanation:	The preventive measures listed in the NIS2 Directive are not much more than a summary of cybersecurity best practices that have been quite commonplace in the security industry for quite some time now. The reason why the legislator has included them explicitly in a legal instrument, is to ensure that more public and private entities effectively implement the things that are considered cybersecurity best practices. One could even argue that the elements listed in Article 21 NIS2 Directive are not that different from the technical and organizational measures which controllers and processors must take to protect personal data pursuant to Article 32 GDPR. The only difference is that the NIS2 Directive is more detailed in the measures which are legally required. The preventive measures can be categorized in four big blocks: 1. Security measures for systems and facilities 2. Measures related to incident handling 3. Measures related to business continuity management 4. Monitoring, auditing, training and testing in relation to the measures mentioned under the previous points. **A. Security measures for systems and facilities** To secure its systems and facilities, the participant must systematically manage its cybersecurity risks by keeping accurate and up-to-date overviews of its IT landscape and putting in place the necessary security policies. The participant must adopt an all-hazards risk-based approach which includes measures aimed at addressing system failure, human error and natural phenomena. Measures are to be taken to address the security of external elements such as network and information system acquisition, development and maintenance and the supply chain. Physical and logical access control must be administrated based on business requirements and policies. The participant should contemplate the use of multi-factor authentication

or continuous authentication solutions and should ensure that voice, video and text communications as well as emergency communications are secured.

B. Measures related to incident handling

The participant must put in place detection procedures and processes and must build up the capabilities required for incident reporting and weakness/vulnerability identification. Incident response procedures and reporting workflows related to the results of the incident response must be implemented. Participants must assess the severity of each incident, document their cybersecurity risk-management related knowledge, collect evidence and put in place continuous improvement processes.

C. Measures related to business continuity management

Participants must draft contingency plans based on business impact analysis which should at least include such topics as back-up management, disaster recovery and crisis management. Backups and backup management, disaster recovery and crisis management capabilities must all be tested to ascertain that the aforementioned contingency plans remain effective over time.

D. Monitoring, auditing, training and testing in relation to the measures mentioned under the previous points

Participants must assess whether network and information systems and their accompanying security measures work as intended. They should perform audits to verify whether standards and guidelines are, and continue to be, complied with, whether records are accurate and targets are met. Processes must be implemented to detect security flaws, basic cyber hygiene practices must become an inherent part of company culture and employees must be trained.

The European Union Agency for Cybersecurity ENISA has developed and published a set of tools which can help participants to comply with the obligations as described above: https://www.enisa.europa.eu/tools.

Question 6:	What notification obligations does a participant have when an incident occurs?
Explanation:	As mentioned in the introduction of this section, Article 23 NIS2 Directive introduces a new process for notifying (significant) incidents as well as cyber threats to the competent authority or the CSIRT (both of which are appointed by the Member State). "Incidents" are defined as "[...] *event*[s] *compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems*". Personal data breaches in the sense of Article 4.12 GDPR are examples of incidents in the sense of Article 6.6 NIS2 Directive. "Cyber threats" are defined as "*any potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other persons.*"[5]

[5] Art. 6.10 NIS2 Directive *jo.* Art. 2.8 Regulation (EU) 2019/881 of 17 April 2019 on ENISA.

Hence, the big difference between an incident and a cyber threat, is that in case of an incident the threat has already materialized, which is not the case when it remains "just" a threat.

The participants must notify incidents which are deemed "significant", i.e. incidents which cause or are capable of causing severe operational disruption of the services or financial loss for the entity concerned OR which have affected or are capable of affecting other natural or legal persons by causing considerable material or non-material damage. Although the practical implementation of the notification mechanism will be up to the individual Member States, the NIS2 Directive already provides the general outline of the notification schema:

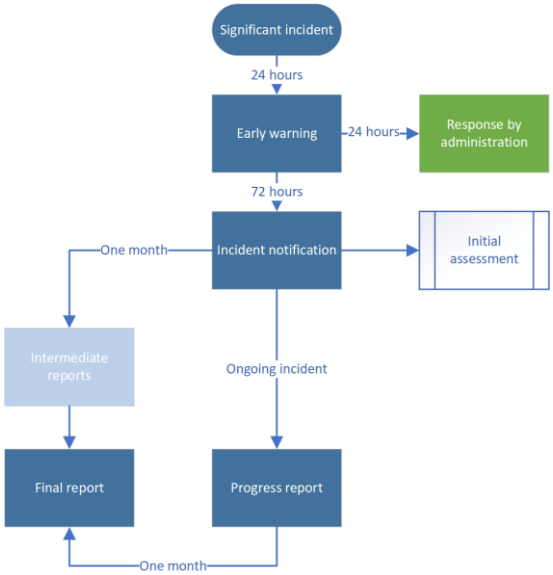

FIGURE 1: NOTIFICATION SCHEMA

Compared with its predecessor, the NIS2 Directive takes a phased approach to notification. It starts with an early warning notification, mainly meant to be quick rather than comprehensive. After that, the participant suffering a significant incident shall perform a more thorough investigation and provide a more complete incident notification, followed by one or more intermediate reports and then a final report. If the significant incident is on-going, the participant shall provide progress reports regarding their handling of the incident.

The participant must also set up a workflow to notify the recipients of measures and remedies that the recipients can take to mitigate the adverse effects of a potential significant cyber threat as well as of the significant threat itself.

Question 7:	Are there particular obligations for the senior management of the participant?
Explanation:	Yes, Article 20 NIS2 Directive demonstrates the EU legislator's intent to give senior management of the entities governed by it a more prominent role and more extensive responsibilities in ensuring an adequate level of cybersecurity.

First of all, the senior management shall have the responsibility to **approve** the cybersecurity measures that are taken by the entity to manage cybersecurity risks.

Secondly, the senior management shall have the responsibility to **oversee** the implementation of the aforementioned measures.

To incentivize senior management to take the aforementioned responsibilities seriously, the EU legislator deemed it necessary to make the management *personally* liable in case of non-compliance by the entity.

The senior management, as well as the employees, must follow training which allows them to identify risks and assess cybersecurity risk-management practices and their impact on the services provided by the entity. While it remains to be seen how the Member States will transpose this obligation, it is clear that it goes well beyond the cybersecurity awareness trainings that one typically finds in most organizations. The knowledge and skills required by Article 20.2 NIS2 Directive indeed hint on the requirement to have more in-depth knowledge than typically gained by common awareness raising trainings which for instance explain the dangers of phishing or what to do when a fraudulent invoice has been received.

3.2 TRUST SERVICES

Trust services were first made subject of a dedicated, comprehensive legal instrument in 2014 with the introduction of the eIDAS Regulation (Regulation (EU) No 910/2014). The eIDAS Regulation's main objective is to foster trust in electronic transactions by setting up a framework for a set of particular services which are at the heart of such transactions and should be trustworthy. It concerns services for the creation, verification and validation of:

- electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services;
- certificates for website authentication;

as well as services for the preservation of electronic signatures, seals or certificates related to the aforementioned services.

The eIDAS Regulation works with a tiered system for providing trust: service providers can choose to provide the aforementioned services as they are, without adhering to (the majority of) the eIDAS Regulation's system of technical requirements, notification, auditing and certification, or they can choose to adhere to that system and become a so-called qualified trust service provider. For electronic signatures and seals there is an intermediate layer, where the service provider adheres to certain additional technical requirements but does not notify, undertake audits or seek certification. This leads to the following tiers: a simple service, advanced service or qualified service. As a service goes up the tiers, it enjoys an increased legal presumption of validity and trust.

In 2021 the European Commission considered that the time was right for an update of the eIDAS Regulation and introduced its proposal for a European Digital Identity Regulation ("EDIR"). The EDIR would not repeal the eIDAS Regulation, but would amend it by adding new trust services. These new trust services are the electronic attestation of attributes and certificates related thereto, the electronic archiving of electronic documents and the management of remote electronic signature and seal creation devices. These new trust services would follow the eIDAS Regulation's tier regime of trust. The European Commission also want to introduce electronic ledgers as a new trust service, but the European Parliament took that out. In addition to these new trust services, the EDIR also introduces the concept of the European Digital Identity Wallet ("EDIW"). The EDIW are electronic means which allow their users to store, manage and validate identity data and the aforementioned electronic attestation of attributes, as well as to provide such data to relying third parties and which allow the creation of electronic signatures

and seals. Providers of an EDIW will have to comply with the eIDAS Regulation as amended by the EDIR. It should be noted, however, that the EDIW as such has not been qualified as a trust service but is merely a "means" to be provided. The EDIR is currently in trilogue negotiations.

Taking into account the scope of the open calls and the current review of the eIDAS Regulation, the obligations and requirements for EDIW and the newly proposed trust service of electronic attestation of attributes and certificates related thereto are the most relevant to be considered in the rest of this section.

Please note that in the remainder of this section, any reference to the "eIDAS 2 Regulation" shall be deemed to refer to the eIDAS Regulation including the amendments proposed in the EDIR as if it had already entered into force. Considering that the EDIR is still a proposal, however, we will use the latest version as was voted upon in the European Parliament and not the European Commission's proposal considering the many changes that were introduced to the latter. The document can be found here: https://www.europarl.europa.eu/doceo/document/A-9-2023-0038_EN.html.

3.2.1 Field of application

Question 1:	When will the eIDAS Regulation apply to the participants?
Explanation:	In accordance with Article 2 eIDAS 2 Regulation, the provisions of the eIDAS Regulation apply whenever the participant offers an EDIW or acts as a trust service provider. The participant would be considered a trust service provider as soon as it provides one of the trust services mentioned in the introduction above. Considering the scope of the open calls, it is not unlikely that participants offer services related to the creation, verification and validation of electronic attestation of attributes or the certificates related thereto. The electronic attestation of attributes is defined in Article 3.44 eIDAS 2 Regulation as "*an attestation in electronic form that allows the presentation and authentication of attributes*", whereas attributes are defined in Article 3.43 eIDAS 2 Regulation as "*a feature, characteristic or quality of a natural or legal person or of an entity*". Participants should bear in mind that the eIDAS 2 Regulation applies as soon as one provides a trust service, irrespective of whether the participant is a qualified trust service provider or not. To be sure, qualified trust service providers must adhere to more obligations and requirements, but that does not mean that non-qualified trust service providers can disregard the eIDAS 2 Regulation altogether.

3.2.2 Registration requirements

Question 2:	Does the participant have to register somewhere to provide regulated services?
Explanation:	Where the participant wants to offer an EDIW, the recitals to the eIDAS 2 Regulation make the EU legislator's intention clear that all issuers of EDIW should be subject to controls and liabilities similar to those of qualified trust service providers. Strangely enough, however, what is currently referred to as Article 6a.9 eIDAS 2 Regulation sets forth that only Member States directly issuing and managing the EDIW shall be subject to (some of the provisions in) Article 24.2 eIDAS 2 Reguation. This is strange for two reasons:

1. it does not refer to private parties whose EDIW is recognized by a Member State, a possibility explicitly added by the European Parliament in Article 6a.2 eIDAS 2 Regulation;
2. it does not refer to the prior registration obligation for trust service providers which is set forth in Article 21 eIDAS 2 Regulation. Of course, if only Member States can be issuers of EDIW, it does not make much sense to include a prior registration obligation, but that does not seem to correspond with what is set forth in Article 6a.2. It remains to be seen what will happen with this in the final version of the EDIR.

It is to be expected that the participant will have to register the EDIW solution, however, considering that the aforementioned Article 6a.2 eIDAS Regulation explicitly states that an EDIW is either issued and managed by the Member State directly OR under its mandate OR independently from the Member State but recognized by it. The latter two options each hint upon the fact that prior registration would be required.

If the participant provides a trust service, then the requirement to register only exists when the participant intends to provide a qualified trust service. Article 21 eIDAS 2 Regulation requires a notification to be made to the competent supervisory authority, accompanied by a conformity assessment.

3.2.3 Legal requirements in relation to the service itself

Question 3: Which requirements are there for providing an EDIW?

Explanation: There are quite a number of legal requirements for EDIW. These requirements relate to user-friendliness, security, data protection, efficiency, cost, technical characteristics, accessibility, interoperability, support, etc. The full list of requirements can be found in Articles 6a to 10a eIDAS 2 Regulation, but we provide a summary for the participants' convenience here:

1. Source code must be open source and published for auditing and review;
2. EDIW must be user-friendly;
3. EDIW should allow online and offline user identification and authentication;
4. EDIW should work for identification and authentication for public and private services;
5. Secure storage, selection, combination and sharing of electronic attestation attributes;
6. Secure issuance and revocation of electronic attestation attributes issued by the user directly;
7. Pseudonym generation, encrypted and local storage;
8. Secure authentication of a third party's EDIW or a relying party;
9. User dashboards providing an overview of all transactions carried out, which allows users to:
    a. View relying parties
    b. Request data deletion from relying parties
    c. Report relying parties to national authorities
    d. Revoke electronic attestations of attributes issued by the user
10. Capability for signing with qualified electronic signatures;
11. Capability for the user to download all of the user's data;
12. Supporting data portability to another EDIW;

13. Using common protocols and interfaces for a number of listed use cases and purposes, such as secure interactions with the electronic identification means of the user and unique, private and secure peer-to-peer connections between EDIW or between an EDIW and a relying party;
14. Ensuring that providers of electronic attestations of attributes cannot technologically access the information of the attributes;
15. Meeting assurance level "high" in relation to electronic identification schemes;
16. When using embedded disclosure policies, ensuring that only EDIW users with the necessary electronic attestation of attribute or the relying party have access to it;
17. Implementing non-repudiation mechanisms for digital requests and transactions;
18. Implementing warning mechanisms to inform users of security breaches;
19. Ensuring that the person identification data representing the natural or legal person is associated with it;
20. Accommodating a user to act on behalf of another natural or legal person;
21. Displaying the EDIW trust mark;
22. Providing technical support to users;
23. Ensuring security-by-design;
24. Issuance and use must be free of charge for the users (which does not mean that an issuer cannot obtain payment from for instance the Member State);
25. Compliance with the technical framework for EDIW, which includes principles such as:
    a. User is in full control;
    b. Using decentralized elements for the identity architecture;
    c. Storage of the electronic identification means, attributes and certificates on the user device, unless the user consents freely to cloud storage;
    d. Allowing secure connections between users and relying parties;
    e. Preventing unauthorized access to identification means, attributes and documents through the technical architecture;
    f. Access to unique and persistent identifiers for relying parties only when allowed by law;
    g. EDIW personal data kept separately from other data held;
    h. Using zero knowledge proofs where identification is not necessary;
    i. Comply with the obligations of controllers under the GDPR;
    j. Provide a complaint mechanism
26. Ensuring accessibility for persons with a disability
27. Complying with the European Commission's reference standards for EDIW
28. Obtaining the necessary certifications for cybersecurity, interoperability and functionality and data protection.

Question 4:	Which requirements are there for providing a trust service consisting of electronic attestation of attributes?
Explanation:	The requirements for the provision of trust services are not as extensive as those for providing an EDIW, especially if the trust service is not qualified. Under Article 15 eIDAS 2 Regulation, the trust services will have to be made available in plain and intelligible language and accessible for persons with disabilities or to

	persons who experience functional limitations, such as older people, and persons with limited access to digital technologies. The old Article 19 eIDAS Regulation is deleted, considering that all trust services must now comply with the NIS2 Directive. As for other trust services, the electronic attestation of attributes cannot be denied legal effect solely on the grounds that it is not a qualified trust service or that it is provided by a provider from another Member State. Notwithstanding this principle, for access to an online service of a public sector body, Member States can require an electronic identification using an electronic identification means and authentication, in which case only qualified electronic attestation of attributes will suffice as an alternative. (Articles 45a and 45b eIDAS 2 Regulation). It will be possible for any trust service provider to issue non-qualified electronic attestations of attributes to an EDIW. Moreover, every provider of electronic attestations of attributes, whether qualified or unqualified, must ensure that a user shall have the possibility to request, obtain, store and manage the electronic attestations of attributes in the EDIW even if that user's EDIW has been issued in a different Member State. It is not allowed to require additional technical, administrative or procedural requirements in such events (Art. 45e eIDAS 2 Regulation). Trust service providers offering electronic attestations of attributes are not allowed to combine personal data related to this trust service with personal data from other services provided by them. Moreover, there must be physical and logical separations in place between the personal data related to the trust service and any other data held and the electronic attestation of attribute services must be provided via separate legal entity (Art. 45f eIDAS 2 Regulation).
Question 5:	Which additional requirements need to be complied with when providing a qualified electronic attestation of attributes?
Explanation:	For those participants wanting to provide qualified electronic attestations of attributes, the requirements are quite a bit more detailed. It starts with the requirement in Article 21 eIDAS 2 Regulation to **notify and providing a conformity assessment** to the competent authority. The conformity relates to the requirements of the eIDAS 2 Regulation but to those of the NIS2 Directive as well. The competent authorities under both instruments must work together, each within its own area of competence, to assess whether the candidate's qualified trust service fulfills the requirements set forth in both instruments. When a trust service provider achieves the qualified status, the provider will be added to the trusted list as foreseen under Article 22 eIDAS 2 Regulation. The qualified trust service providers must also, at their own expense, undergo **audits** every 24 months by a conformity assessment body (Article 20 eIDAS 2 Regulation). In case the audit finds potential violations of the GDPR, the data protection authorities will be informed. If non-conformities are detected, the trust service provider will get a period to remedy the situation. If the remedy was not adequate or not implemented, the competent authority can revoke the qualified status. When issuing a qualified electronic attestation of attributes, the qualified trust service provider must verify the identity and any specific attributes of the natural or

legal person (Art. 24.1 eIDAS 2 Regulation). There are four ways the qualified trust service provider can do this:

1. Using electronic identification means with assurance level "high";
2. Using a certificate of a qualified electronic signature or seal;
3. Using other identification methods facilitating identification with a high level of confidence (conformity must be confirmed by the conformity assessment body);
4. Through physical presence of the person.

Article 24.2 eIDAS 2 Regulation adds a whole additional list of requirements to be complied with by the qualified trust service provider, including in relation to informing the competent authority of changes, adequate staff and supplier management, adequate financial resources, clear terms and conditions, trustworthy systems and products, adequate risk management practices, security measures, data availability after service cessation, service continuity planning and compliance with data protection law.

On top of the aforementioned requirements, qualified electronic attestation of attributes requires compliance with the following technical measures, to which Member States cannot add additional ones for the trust service provider to obtain the qualified status (see Annex V):

(a) an indication, at least in a form suitable for automated processing, that the attestation has been issued as a qualified electronic attestation of attributes;
(b) a set of data unambiguously representing the qualified trust service provider issuing the qualified electronic attestation of attributes including at least, the Member State in which that provider is established and:
    a. for a legal person: the name and, where applicable, registration number as stated in the official records,
    b. for a natural person: the person's name;
(c) a set of data unambiguously representing the entity to which the attested attributes is referring to; if a pseudonym is used, it shall be clearly indicated;
(d) the attested attribute or attributes, including, where applicable, the information necessary to identify the scope of those attributes;
(e) details of the beginning and end of the attestation's period of validity;
(f) the attestation identity code, which must be unique for the qualified trust service provider and if applicable the indication of the scheme of attestations that the attestation of attributes is part of;
(g) the qualified electronic signature or qualified electronic seal of the issuing qualified trust service provider;
(h) the location where the certificate supporting the advanced electronic signature or advanced electronic seal referred to in point (f) is available free of charge;
(i) the information or location of the services that can be used to enquire about the validity status of the qualified attestation.

Qualified providers of electronic attestations of attributes must provide interfaces to EDIW. They shall also comply with the data protection limitations set forth in Article 45f eIDAS 2 Regulation as explained above for non-qualified trust service providers.

3.3 OTHER INSTRUMENTS

The previous sections give a bit more in-depth guidance to legal and regulatory topics which can be presumed to be highly relevant to the open call participants. There are, however, quite a few other topics which may be of relevance, depending on the anticipated activities of the participants, such as the Digital Services Act (Regulation (EU) 2022/2065), rules on e-commerce and consumer protection and intellectual property law. A very brief introduction to each of these topics can be found in this section.

3.3.1 Digital Services Act

Instrument:	The Digital Services Act (Regulation (EU) 2022/2065) entered into force at the end of 2022 and will start to apply on 17 February 2024. The Digital Services Act is a regulation and will not require transposition in Member State law.
Objective:	The main objective of the Digital Services Act is to amend the E-Commerce Directive in such a way that on the one hand a uniform legal framework emerges for intermediary services in the European Union, while on the other hand the safety of the online environment is improved by imposing due diligence and transparency obligations on those intermediary services.
Personal scope:	The provisions of the Digital Services Act apply to providers of intermediary services, with additional obligations for online platforms and very large online platforms. An online platform is "*a hosting service that, at the request of a recipient of the service, stores and disseminates information to the public, unless that activity is a minor and purely ancillary feature of another service or a minor functionality of the principal service and, for objective and technical reasons, cannot be used without that other service, and the integration of the feature or functionality into the other service is not a means to circumvent the applicability of this Regulation*" None of the participants qualify as very large online platforms, so that will not be further covered.
Material scope:	The Digital Services Act targets "intermediary services", meaning one of the following services: - 'mere conduit' service, *consisting of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network*; - 'caching' service, *consisting of the transmission in a communication network of information provided by a recipient of the service, involving the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information's onward transmission to other recipients upon their request*; - 'hosting' service, *consisting of the storage of information provided by, and at the request of, a recipient of the service*. Intermediary services are provided to a recipient of the service, which is "*any natural or legal person who uses an intermediary service, in particular for the purposes of seeking information or making it accessible.*" As with the E-Commerce Directive, the Digital Services Act will apply in both B2B and B2C relationships.

Territorial scope:	The Digital Services Act will apply when the recipients of an intermediary service have their place of establishment or residence in the European Union, irrespective of where the provider of the intermediary service has its place of establishment.
Key obligations:	The main obligations of providers of intermediary services or online platforms under the Digital Services Act are: - to act against illegal content when receiving an order issued by competent national judicial or administrative authorities ("illegal content" means "any information, which, in itself or by its reference to an activity, including the sale of products or provision of services is not in compliance with Union law or the law of a Member State, irrespective of the precise subject matter or nature of that law"); - to provide information on or about recipients of the intermediary service in response to an order issued by competent national judicial or administrative authorities; - to appoint a point of contact for authorities; - to include mandatory information in terms and conditions; - to report yearly on content moderation activities; - to put in place notice and action mechanisms. Online platforms must also set up internal complaint handling mechanisms and allow for out-of-court dispute settlement. They must handle notices submitted by trusted flaggers with priority, take measures against misuse and notify suspected serious criminal offences. If the online platform allows distance contracts to be concluded between traders and consumers, it must collect information on the traders. Online platforms also have dedicated transparency reporting and online advertising transparency obligations.
Enforcement:	The Member State competent for enforcement is the Member State where the provider of the intermediary service or the online platform has its main establishment or its representative. The Member States will appoint so-called "Digital Services Coordinators" which will be responsible for the enforcement of the provisions of the Digital Services Act in a Member State. They will have powers of investigation, of enforcement and even the power to impose the obligation on management to take measures or to request interventions by judicial authorities.

3.3.2 E-commerce and consumer protection

Instrument:	The main instruments in this domain are, at the European level, the E-commerce Directive (Directive 2000/31/EC), the Digital Content and Services Directive (Directive (EU) 2019/770) and the Consumer Rights Directive (Directive 2011/83/EU). Considering that all of these instruments are directives, all of them have to be transposed in national law.
Objective:	The main objective of the E-commerce Directive is to strengthen the e-commerce sector in the EU through harmonisation of rule of establishment, transparency obligations, rules on marketing communications and liability exemptions.

	The main objective of the Digital Content and Services Directive is to protect consumers when buying digital products and services online by introducing conformity requirements and allocating liability to traders offering such content and services. The main objective of the Consumer Rights Directive is to protect consumers when buying goods and services by introducing detailed rules on transparency towards consumers and introducing additional rights (such as the right to withdrawal).
Personal scope:	The provisions of the E-Commerce Directive, and the national transposition thereof, apply to a "service provider" which is "*any natural or legal person providing an information society service*". The provisions of the Consumer Rights Directive and the Digital Content and Services Directive apply to a "trader" which is "*any natural or legal person, irrespective of whether privately or publicly owned, that is acting, including through any other person acting in that natural or legal person's name or on that person's behalf, for purposes relating to that person's trade, business, craft, or profession, in relation to contracts covered by this Directive*".
Material scope:	The E-Commerce Directive targets "information society services" which are "*services normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services.*" The provisions apply irrespective of whether the information society service is provided to a consumer or another recipient of the service (so both B2C and B2B). The Digital Content and Services Directive targets digital content and digital services provided to consumers (so only B2C). "Digital content" are "*data which are produced and supplied in digital form*". A "digital service" is "*a service that allows the consumer to create, process, store or access data in digital form or a service that allows the sharing of or any other interaction with data in digital form uploaded or created by the consumer or other users of that service.*" The Consumer Rights Directive targets contracts with consumers which are concluded at a distance or off-premise as well as other contracts (so only B2C). For the purposes of this deliverable, only the distance contracts would seem relevant, which are contracts "*concluded between the trader and the consumer under an organised distance sales or service-provision scheme without the simultaneous physical presence of the trader and the consumer, with the exclusive use of one or more means of distance communication up to and including the time at which the contract is concluded.*"
Territorial scope:	The E-Commerce Directive applies when the provider of an information society service is established within the European Union. The Consumer Rights Directive and the Digital Content and Services Directive apply when the trader providing digital content or digital services is subject to the laws of a European Member State (e.g., due to its establishment).
Key obligations:	The main obligations of service providers under the E-Commerce Directive, are: - to provide certain information regarding the service provider; - to provide certain information regarding the ordering process and the contract; - to implement the ordering process in a particular way;

- to confirm orders;
- to comply with certain requirements regarding advertising and commercial communications;
- to observe certain requirements for contracts concluded through electronic means.

The main obligations of traders under the Consumer Rights Directive are:

- to provide certain information to the consumer before that consumer is bound by the agreement for goods or services;
- to provide the consumer with the information on a durable medium;
- to observe the right to withdrawal where it applies.

The main obligations of traders under the Digital Content and Services Directive are:

- to start with the delivery of the content or service without undue delay after conclusion of the contract;
- to ensure the conformity of the digital content or service, which entails both objective and subjective requirements;
- to take responsibility for violations of third parties;
- to bear the liability in case of failure to supply or non-conformity;
- to bear the burden of proof;
- to observe certain obligations in case of termination of the agreement.

3.3.3 Intellectual property law

It seems very likely that participants, as a result of their participation to the open calls, will generate results which are protected or protectable through intellectual property rights. Below we provide a succinct first introduction to different regimes for protecting intellectual property.

3.3.3.1 Different types of intellectual property rights

There are several different intellectual property regimes depending on the type of intangible item the ownership of which needs protecting. The first regime is that of copyright: the rules that regulate the creation and use of a range of cultural goods such as books, computer programs, photos, films etc. A second regime is that of patents: the protection of inventions which can be described in technical information. A third regime is that of designs: the protection of the appearance of the whole or a part of a product. A fourth regime is that of trademarks: the protection of graphically representable signs that are capable of distinguishing goods or services from those of someone else.

Each of these regimes are very distinct on how one can apply for protection, the subject matter of what can be protected, the scope of protection, the duration of protection and how the right can be exploited. We would venture that copyright, patent protection and trademarks are the relevant regimes to be considered by most participants. In what follows we will highlight how each regime may be relevant to participants' solutions and products.

3.3.3.2 Protection via copyright

Copyright is arguably one of the most important regimes for protecting intellectual property rights in the context of the open calls. Copyright can be applied to a great many things, including software and publications. It seems more than likely that part of the participants' results will be new software applications. Copyright is therefore one of the more important regimes to be discussed. The rules on copyright are mainly found in the national Member State law, but also in international treaties such as

the Berne Convention, Trade-Related Aspects of Intellectual Property Rights Agreements (TRIPS Agreement) and a number of European directives (e.g. InfoSoc Directive (2001/29/EC), Computer Programs Directive (2009/24/EC) and the Database Directive (96/9/EC)).

Copyright protects literary works, scientific works as well as works of art. Included in these broad categories are computer programs as per the Software Directive and databases as per the Database Directive. Important to note is that computer programs include source code, assembly code and object code but not the GUI. With regard to databases, the protection via copyright is aimed at the systematic or methodical arrangement of the content in a database and not at the content (e.g. raw data) itself. This does not mean that there is no protection for the content of the database itself, but then one has to go through the special protection regime that exist for databases. The scope of protection of that special regime is limited to where there has been a substantial investment in obtaining, verifying, or presenting the contents of a database. Note that the substantial investment in the creation of the contents is not relevant. This makes it fairly difficult in practice to use the special database protection regime.

Under copyright the ownership lies with the author. For the special database protection regime, the owner is the person who takes the initiative in obtaining, verifying or presenting the contents of a database and who runs the risk of the investment. It is important to note that ownership under copyright law does not require any prior registration. Copyright vests in the author at the moment of creation of the work, without any official authority granting the copyright. It directly stems from the applicable copyright law itself. Protection in the EU is granted for the duration of the life of the author plus seventy years for works protected by copyright. For databases protected under the special database protection regime, duration of protection is limited to fifteen years.

3.3.3.3 Protection via patents

Patent protection is granted to inventions via again a multilayered legal framework composed of international and national legal instruments. The most important are the European Patent Convention, the TRIPS Agreement and national patent laws. While there are many types of patents, we believe that if patents will be considered through patents – which is less likely than seeking protection under copyright – it will be product claims or process claims. Product claims pertain to seeking patent protection for a product, i.e. a device. Process claims pertain to seeking patent protection for a process. While there are clear economic benefits associated with patents, the disadvantage is that the invention is made public to the world and that they are quite expensive to obtain. As a rule of thumb, the decision to patent should be linked to the cost of copying: the higher the cost of copying the more appropriate it is to rely on secrecy instead of a patent. If a patent is granted, it offers protection for twenty years.

Contrary to copyright protection the protection through patent law is not granted automatically. It does not vest immediately in the creator of an invention the moment of its conception. If a participant wishes to seek protection through patents, he will need to apply for a patent with the national patent office or with the European Patent Office. The person who is first to submit a valid patent application for an invention, is granted the patent.

Not every invention, be it a product or a process, is patentable. First, the invention must have a concrete and technical character so that it is capable of industrial application. Second, the invention cannot be a discovery, scientific theory, mathematical method, works protectable through copyright and the presentation of information. Third, the invention must be novel taking into account its characteristics versus the state of the art. Fourth, the invention must include an inventive streak: it should not be obvious to a person skilled in the art.

There are also very strict requirements regarding how a patent should be drafted. If an invention made during participation to the open call is patentable, the respective participant would do well to seek specialized assistance for filing for patent.

3.3.3.4 Protection via trade marks

Trade mark protection in the EU is largely determined by European law, more specifically by the Trade Mark Directive (Directive 2008/95/EC, replaced by Directive (EU) 2015/2436) and the Community Trade Mark Regulation (Regulation (EC) 207/2009). National law is also relevant of course, since the aforementioned Trade Mark Directive needs to be transposed. As with patents, the protection of a trade mark follows from its registration. An application of a trade mark can be locally with a national registrar, at the level of the EU (through an institute called OHIM) for a community trade mark or internationally with the WIPO (the application goes through the national registrar).

A trade mark is a sign that can be represented graphically, which means using images, lines or characters. The trade mark must also be capable to distinguish from the services of someone else, i.e. it must be distinctive. The term of protection granted by a trademark is usually ten years.

4 CONCLUSIONS

This deliverable has mapped out the different ethical and legal instruments which are most likely to apply to all projects proposed under the open calls and provides participants with guidance on what they have to do to comply with them. This deliverable only provides an introduction, however, and cannot replace precise ethical and legal advice concerning the impact of each of these instruments. Hence, participants should use this deliverable as a tool to understand what they have to do, but should subsequently apply the insights provided herein to their own concrete case. This may require further ethical and legal support, which can be provided through the TrustChain consortium.

APPENDIX A

Consent Form - Processing of personal data in [Project Name]

[Name participant1], [address] AND [Name participant1], [address]; together referred to as "the parties" or "we" and each responsible for the processing of your personal data; would like to process your personal data as described below, [optional: including data concerning health,] for the purposes of research and development as part of a knowledge transfer experiment set up in the context of the project "[Name Project]". The personal data will also be anonymized to be used in scientific publications and to be made available in an open data repository.

Your personal data are processed solely on the basis of your consent. With this form, the parties wish to ask you for such consent. It is not possible to participate to the project without your consent, because we would not be allowed to collect and analyse the data related to your participation. You can withdraw your consent at any time.

Types of personal data which we process are: [add personal data categories].

Your personal data will be stored for [add retention period] after the receipt of your consent or until such time when you withdraw your consent, whatever comes first. Your personal data will be stored in the European Economic Area.

Your personal data will be accessible to you, the parties and IT service providers whose services are used by the parties. When anonymized, data will be accessible to anyone who has access to the open data repository.

You have the right to request access to all personal data pertaining to you that we process. You have the right to ask that any personal data pertaining to you that are inaccurate, are corrected free of charge. You have the right to request that personal data pertaining to you be deleted if these data are no longer required in the light of the purposes outlined above or if you withdraw your consent for processing the data. Instead of deletion you can also ask that we limit the processing of your personal data if (a) you contest the accuracy of the data, (b) the processing is illegitimate, or (c) the data are no longer needed for the purposes mentioned above. You have the right to receive from us in a structured, commonly-used and machine-readable format all personal data which you have provided to us. If you wish to submit a request to exercise one or more of the rights mentioned above, you can send an e-mail [add email address]. If you have any complaint regarding our processing of your personal data, please feel free to contact us using the aforementioned email address. Should you remain unsatisfied with our response, you have the right to file a complaint with the competent supervisory authority.

To be completed by you, the participant:

Name: .....

☐ **I give my permission to process my personal data as described herein.**

☐ **I give my explicit and unambiguous permission to process my data concerning health as described herein.**

□ **I understand and agree that the copyright and any other intellectual property which arises in the photographs in which I feature belongs to parties and that I will not receive any reimbursement for the right to take or to use such photographs.**

I certify that I have read and fully understand this consent and release and that all questions pertaining to this consent have been answered to my satisfaction.

Date: ..... Signature: .....