D2.11

Legal, Ethical and Societal Requirements and Constraints

Document Identification	
Date	30.11.2019
Status	Final
Version	1.1

Related WP	WP2	**Related Deliverable(s)**	D2.9, D2.3, D3.2., D.2.6, D2.10
Lead Authors	Hans Graux (TIL)	**Dissemination Level**	PU
Lead Participants	TIL, FHG	**Contributors**	FHG, TIL
Reviewers	OIX, TUG		

This document is issued within the frame and for the purpose of the LIGHT*est* project. LIGHT*est* has received funding from the European Union's Horizon 2020 research and innovation programme under G.A. No 700321.

1. Executive Summary

The LIGHTest project must be executed in accordance with applicable laws, ethical standards, and societal constraints. Compliance with data protection law is a central concern, in particular the General Data Protection Regulation (EU) 2016/679 (GDPR), which became applicable on 25 May 2018 (i.e. in the course of the LIGHTest project). In addition, LIGHTest use cases need to take into consideration potential national data protection laws where the GDPR still leaves a margin of appreciation to the Member States (e.g. when LIGHTest would be used for the processing of data concerning health, or for scientific research purposes).

Data protection issues are explored in greater detail in deliverables D1.2 and D1.3, as a part of the definition of ethical compliance approaches, and also in D2.1 - Requirements and Use Cases, which already identified privacy related requirements. In this deliverable, we explain how data protection challenges can be identified and mitigated effectively by conducting data protection impact assessments (DPIAs), as is foreseen in the GDPR. Data protection challenges are thus discussed in Chapter 4 of this deliverable.

Beyond data protection, other legal constraints apply as well. Most visibly, the LIGHTest project is being executed against the legal backdrop of the eIDAS Regulation, i.e. Regulation 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. The eIDAS Regulation specifically applies to the Trustworthy Communication Services Pilot, but will be relevant to any use case requiring electronic signatures or electronic identification via LIGHTest infrastructure. Thus, compliance with the eIDAS Regulation will be critical for ensuring the viability of the project outcomes in general.

But legal, ethical and societal requirements do not end with data protection law and eIDAS compliance (which are discussed in Chapter 4 of this deliverable). In order to correctly appreciate the challenges that LIGHTest faces, it is important to recognise that LIGHTest provides a technology for publishing, validating and translating trust information. As a technology, the surrounding compliance challenges depend on the use cases: while certain compliance factors (such as data protection and eIDAS compliance) can be built into the technology to a certain extent, the legal, ethical and societal requirements are largely dictated by use cases and the standards that apply to these. By way of a practical example: using LIGHTest to validate whether an eSignature is trusted is very different from using LIGHTest to determine whether a passenger is a criminal whose entry into a country is permitted.

For the avoidance of doubt, the latter use case is not piloted in LIGHTest, but the example illustrates that the legal, ethical and societal assessment of technologies depend very much on their usage. Defining abstractly how a technology complies with laws in all cases is not possible. However, it is possible to define an analytical framework that allows legal challenges for LIGHTest use cases to be identified. This deliverable defines legal, ethical and societal requirements by

creating such a legal assessment framework, which can thereafter be applied to pilot usage scenarios, in order to identify and address their specific legal challenges.

In order to fulfil this goal, this deliverable firstly identifies key legal principles with a basis in EU law, in order to identify the requirements that should be assessed in any use case of the LIGHTest technology. Thereafter, it creates a legal assessment framework that integrates the resulting legal, ethical and societal requirements and allows the resulting barriers and challenges to be identified in any LIGHTest use case (Chapter 5 of this deliverable).

Methodologically, this was done by evaluating relevant EU level legal texts at the general level – i.e. without going into the legislation governing individual use cases or specific pilot contexts – and attempting to extract or derive general principles that will need to be adhered to when applying the LIGHTest technology.

Key source documents were the EU Charter of Fundamental Rights, the Universal Declaration of Human Rights, the Data Protection Directive, the APEC Privacy Framework, the General Data Protection Regulation, the eIDAS Regulation, the UNCITRAL Model Law on Electronic Signatures, the e-Commerce Directive, the UNCITRAL Model Law on Electronic Commerce, and the United Nations Convention on the Use of Electronic Communications in International Contracts. While not comprehensive, this regulatory package was selected in order to extract legislation that was most likely to impact LIGHTest use cases and that would be useful in order to identify internationally applicable and relevant legal, ethical and societal principles.

This is not a theoretical or academic exercise: the legal assessment framework created in this deliverable is designed to be used in practice to execute domain-specific analyses for specific piloting use cases. This deliverable explains how this principle can be applied in Chapter 6, where the legal assessment framework is applied to the LIGHTest use cases. The outcome is a statement of legal, ethical and social requirements that must be satisfied in order to implement LIGHTest technology in a specific use case.

Of course, LIGHTest must not only identify legal requirements, but also potential solutions. This has however been done in the quartet of related compliance deliverables:

- D3.7 - Cross-Border Legal Compliance and Validity of Trust Scheme Publication explains the legal challenges behind the publication of trust schemes and the need for a trust framework (through laws or contracts) that explains the legal assurances and guarantees behind the publication.
- D4.7 - Cross-Border Legal Compliance and Validity of Trust Scheme Translation explains the legal challenges behind the translation of trust schemes, including the need to publish terms under which the translation can be done (via a law or treaty, or simply via a contract).
- D5.7 - Cross-Border Legal Compliance and Validity of Delegation explains the legal challenges behind creating and managing delegations, including the focus on data quality (creation, validation, keeping it up to date, and liabilities behind it).

- D6.8 - Cross-Border Legal Compliance and Validity of Trust Policy and Trust Decisions explains how this infrastructure is used in practice to support decision making.

This deliverable was drafted on the basis of D2.10 - Legal, Ethical and Societal Requirements and Constraints (v1), but has been updated based on the experiences in the pilots, in order to ensure the long-term usability of LIGHTest outputs and lessons learned. For this reason, particular attention has been paid to data protection impact assessments as key tools to mitigate ethical and societal issues, and data protection related legal issues.

In this manner, LIGHTest can ensure that legal, ethical and social requirements are fully complied with for the duration of the project. Even after the conclusion of the project, the assessment framework and the guidance on DPIA usage will ensure that any third parties that wish to use LIGHTest's infrastructure can easily do so in full compliance with applicable requirements.

2. Document Information

2.1 Contributors

Name	Partner
Hans Graux	TIL

2.2 History

Version	Date	Author	Changes
1.0	12.11.2019	TIL	First draft

3. Table of Contents

3.1 Table of Figures

3.2 Table of Tables

N.A.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

4. Central legal requirements – data protection law and the eIDAS Regulation

4.1 Introduction – the importance of data protection law and the eIDAS Regulation for LIGHTest

The LIGHTest project proposal indicated two legal texts as being the crucial sources of legal, ethical and social requirements: on the one hand, the eIDAS Regulation (governing electronic identification and trust services), and on the other hand data protection law (historically and at the beginning of the project the Data Protection Directive 95/46/EC (hereafter the 'DPD'[1]), and since 25 May 2018 the General Data Protection Regulation (EU) 2016/679 (hereafter the 'GDPR')[2].

These two sources are indeed critical for the pilots that are envisaged within LIGHTest and for its further use after the completion of the project:

- Firstly, the eIDAS Regulation provides the legal framework for the mutual recognition of notified means of electronic identification and for the cross-border validity of certain trust services, including electronic signatures, seals, time stamps and electronic delivery services. Electronic identification and trust services are key building blocks to information security: as argued in greater detail in D2.9 (the Social Impacts Report), they are critical enablers of security in any electronic transaction, and the potential beneficial social impact of using LIGHTest to support them is vast: trust services and electronic identities can be better leveraged while fully respecting national sovereignty on this point, international business transactions can be better secured as can e-government services and even citizen-to-citizen communications, innovation can be spurred and economic growth supported.
- Secondly, European data protection law (historically national transpositions of the DPD, and since 25 May 2018 the General Data Protection Regulation) governs how personal

[1] 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; see http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML; last visited on 15 May 2017

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation); see http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32016R0679; last visited on 15 May 2017

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

data must be processed in any context, and therefore also applies when using the LIGHTest technology in use cases involving the processing of personal data. Compliance with data protection law is particularly crucial to LIGHTest: at its heart, LIGHTest uses a global technology (the DNS) for the publication, validation and translation of trust information. If this implies that personal data is processed via the DNS, this would raise significant compliance challenges that must be mitigated, especially since data within the DNS must be publicly accessible. In other words, a misapplication or misconfiguration of LIGHTest could have negative repercussions on persons whose data is being processed, or at least create significant compliance burdens for users of the LIGHTest technology.

Thus, the focus of the LIGHTest proposal on compliance with data protection law and the eIDAS Regulation is justified. None the less, legal, ethical and societal requirements in LIGHTest do not end with data protection law and eIDAS compliance (although these will indeed be central to the current Chapter 4). In order to correctly appreciate the legal, ethical and societal challenges that LIGHTest faces – or rather, that users of LIGHTest technology will face - it is important to recognise that LIGHTest provides a technology for publishing, validating and translating trust information. This can trigger additional compliance burdens outside the context of data protection or eIDAS.

As a neutral technology, the surrounding compliance challenges depend on the use cases: while certain compliance factors (such as data protection and eIDAS compliance) can and will be built into the technology to a certain extent, the legal, ethical and societal requirements are largely dictated by use cases and the standards that apply to these. By way of a practical example: using LIGHTest to validate whether an eSignature is trusted is very different from using LIGHTest to determine whether a passenger is a criminal whose entry in a country is permitted. Or more trivially: whether LIGHTest can be used to validate an electronic order depends largely on eCommerce laws, rather than data protection or the eIDAS Regulation.

For the avoidance of doubt, the latter use cases are not piloted in LIGHTest, but the example illustrates that the legal, ethical and societal assessment of technologies depend very much on their usage. Defining abstractly how a technology complies with laws in all cases is not possible. This is why this deliverable is not limited to data protection and eIDAS compliance; the following chapter will explore other legal, ethical and social requirements and how they impact LIGHTest use cases.

Firstly however, the sections below will examine in greater detail how data protection law and the eIDAS Regulation will affect LIGHTest, and which compliance measures can and should be built in.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

4.2 Personal data and data protection law in LIGHTest

4.2.1. Data protection law in general

The LIGHTest project must be executed in accordance with the highest legal and ethical standards, including in particular with respect to data protection law. Any processing of personal data must therefore comply with applicable data protection law, historically national transpositions of the Data Protection Directive (DPD), and since 25 May 2018 the GDPR. This deliverable will focus principally on the GDPR rather than the DPD in order to safeguard its future usefulness.

As was explained in greater detail in D1.2 – NEC Requirements, the GDPR applies to the processing of any personal data, i.e. to any information relating to an identified or identifiable natural person (a 'data subject'), that will take place via the LIGHTest infrastructure (article 4 (1) of the GDPR). This implies a need to assess whether the data processed within LIGHTest constitutes 'personal data' as defined in these laws, i.e. whether it permits a specific natural person to 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 (article 4.1 of the GDPR).

As described more specifically in D3.2 - Conceptual Framework for Trust Schemes (2), in D2.3 - Requirements and Use Cases, and in D2.6 - Formal Description and Analysis of Concepts (3), LIGHTest inherently relates to the publication, validation and translation of (repositories of) trusted information through DNS infrastructure, and on enabling decision making on the basis of this information. If that information directly or indirectly permits a specific natural person (a human) to be identified, then LIGHTest is indeed used to process personal data, and data protection law must be complied with.

For the purposes of LIGHTest, the publication of directly identifiable information within the DNS system using LIGHTest components would certainly qualify as processing of personal data; an example would be the publication of identity information (name, job title or contact information) of a person authorised to represent a certain organisation. Indirectly identifiable information would however also qualify, e.g. through the publication of a pseudonymous identifier that might not permit the identification of a natural person as such, but which could permit the identification of that person in combination with other information. An example would be the publication of a unique identity number within the DNS system of a person authorised to represent a certain organisation.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

In relation to LIGHTest, the conclusion is clear: if any data is published within the DNS system that permits the direct or indirect identification of a natural person, data protection law will apply.

In such cases, a data controller must be identified, i.e. the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data (article 4.7 of the GDPR). In the context of LIGHTest pilots, the controller would typically be either a legal entity (e.g. a company, organisation or public body) participating in LIGHTest, or a group of such entities (including potentially the LIGHTest consortium as a whole).

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

4.2.2. Data protection compliance requirements in LIGHTest

When data protection law applies – either in the form of the GDPR or in the form of national laws complementing the GDPR – a series of formal compliance requirements for the processing of personal data must be respected.

The resulting data protection compliance requirements have already been identified in D2.3, in order to ensure that the deliverable could be read on its own as a standalone document. This was done by screening the text of the DPD and the GDPR to extract core principles and obligations:

No.	PR-01.00- Privacy by design
Description	The LIGHTest project MUST protect any personal data it collects or processes according to the definition of personal data in the GDPR and any data controllers of such personal data within LIGHTest MUST, both at the time of the determination of the means for processing and at the time of the processing itself, 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 GDPR and protect the rights of data subjects.

No.	PR-01.01- No revocable privacy
Description	Actors MUST NOT be subject to any mechanism that revokes their privacy. This includes backdoors, key-escrow or similar concepts that ultimately places control of an actor in the hands of a third party.

No.	PR-02.00- Privacy by default
Description	Any personal data Controller within LIGHTest boundaries MUST 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. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility.

No.	PR-02.01- Privacy-friendly settings
Description	As a corollary of the Privacy by default requirement, all preferences, configuration, and other settings, SHOULD use the most privacy-friendly settings as the default settings, where technically feasible in a compatible way with the use of existing

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

	DNSSEC technology. Changes from the defaults and their implications on users' privacy SHOULD be both clearly documented and conveyed to the actor making the change.

No.	PR-03.00- Unlinkability
Description	The Pilots using Components of the LIGHTEST Reference Architecture MUST support the privacy protection goal of unlinkability. They MUST ensure that privacy-relevant data cannot be linked across privacy domains that are constituted by a common purpose and context.

No.	PR-03.01- Purpose limitation (lawfulness and fairness)
Description	Any personal data SHOULD be collected only for specified, explicit, lawful, and fair purposes and not further processed in a way incompatible with those purposes. The personal data SHOULD be adequate, relevant and limited to what is necessary for the purposes for which they are processed. In particular, the specific purposes for which personal data are processed SHOULD be explicit and legitimate and determined at the time of the collection of the personal data.

No.	PR-03.02- Sensitivity awareness
Description	Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation MUST be prohibited, unless one of the conditions listed in Article 9 of the GDPR applies.

No.	PR-04.00- Data minimisation
Description	Any personal data collected MUST be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed

No.	PR-04.01- Minimal registration data
Description	As a corollary of the data minimisation requirement, any data required to use the LIGHTest services by any actor SHOULD NOT include any identifiable data, and any identifier SHOULD be randomly generated.

No.	PR-04.02- Limited storage time

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

Description	Any personal data collected MUST be kept in a form which permits identification of the owner for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) of the GDPR subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of the data subject.

No.	PR0-5.00- Transparency
Description	Any personal data collected MUST be processed in a transparent manner in relation to the Data Subject: information MUST be provided to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed. Natural persons SHOULD be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing.

No.	PR-05.01- Owner explicit delegation
Description	When a delegation process is implemented, actors MUST explicitly be involved in it.

No.	PR-05.02- Limited re-delegation
Description	Delegations SHOULD NOT be delegatable in turn, unless strictly required by the nature of the service provided and with the consent of the original actor.

No.	PR-05.03- Transparent delegation overlap
Description	When being informed about a delegation request, actors SHOULD explicitly be warned, if applicable, if any part of the LIGHTest pilot that the delegation requests concern, is already the subject of delegation.

No.	PR-05.04- Transparency towards actors
Description	All outcomes of authentication, authorization, delegation, and identity and attribute management processes, including any automated decision-making, MUST be visible (transparent) for the relevant actor whose electronic transaction is being processed.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

No.	PR-05.05- Notification
Description	If personal data are obtained from the Data Subject, the Data Controller MUST provide the Data Subject with the information described in Article 13 of the GDPR. If any personal data have not been obtained from the Data Subject, the Data Controller MUST provide the Data Subject with the information described in Article 14 of GDPR. The controller MUST communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with Articles 16, 17(1) and 18 of GDPR to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller MUST inform the Data Subject about those recipients if the Data Subject requests it.

No.	PR-06.00- Intervenability
Description	The Pilots using Components of the LIGHTEST Reference Architecture MUST support the privacy protection goal of intervenability. Data subjects MUST be provided with the opportunity to have control over how their personal data is processed.

No.	PR-06.01- Right to be forgotten
Description	If any personal data are collected, the owner MUST have the right to obtain from the Data Controller the erasure of personal data concerning her/him without undue delay and the Data Controller MUST have the obligation to erase personal data without undue delay, if any of the grounds from Article 17 of the GDPR applies.

No.	PR-06.02- Right to restriction of processing
Description	The owner MUST have the right to obtain from the Data Controller the restriction of the processing of personal data, if any of the grounds from Article 18 of the GDPR applies.

No.	PR-06.03- Right to object
Description	The Data Subject MUST have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on points (e) or (f) of Article 6(1) of the GDPR, including profiling based on those provisions. The Data Controller MUST no longer process the personal data unless the Controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

No.	PR-06.04- Right to data portability

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

Description	The Data Subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a Data Controller, in a structured, commonly used and machine-readable format and have the right to transmit that data to another Controller without hindrance from the Controller to which the personal data have been provided, where the conditions specified in Article 20 of the GDPR are met.

No.	PR-07.00- Accuracy
Description	Any personal data collected MUST be accurate and, where necessary, kept up to date; every reasonable step MUST be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, will be erased or rectified without delay.

No.	PR-08.00- Storage trustworthiness and accountability
Description	If any personal data is collected for the LIGHTest pilots, the pilots MUST provide a trustworthy storage for them preserving their authenticity, where only authorized persons would be allowed to make changes and new entries. Each Data Controller and, where applicable, the controller's representative, MUST maintain a record of processing activities under its responsibility. That record shall contain all of the information specified in Article 30 of GDPR.

No.	PR-09.00- Integrity and confidentiality
Description	Any personal data collected MUST be processed in a way that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage; the Data Controller MUST implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, and when a personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the Data Controller MUST communicate the personal data breach to the Data Subject without undue delay.

No.	PR-09.01- Anonymization for statistics
Description	Data SHOULD be anonymized, if applicable, prior to being processed for statistical analysis

No.	PR-09.02- Key privacy
Description	If a public-key encryption scheme is implemented, it should provide key privacy if applicable. Key privacy is a security property of public-key encryption algorithms that

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

	requires that ciphertexts produced by an encryption algorithm do not leak any information about which public key was used to produce the ciphertext.

No.	PR-09.03- Private process outcomes
Description	Information on all process outcomes SHOULD NOT be available to anyone else, unless required by the nature of the service provided and with the consent of the original actor.

No.	PR-09.04- Private metadata
Description	The metadata used to reference encrypted data stored in the LIGHTest pilots SHOULD NOT reveal information regarding the actors.

No.	PR-09.05- Private policies
Description	Authorization and delegation policies/preferences stored in LIGHTest SHOULD NOT reveal information regarding the actors.

No.	PR-10.00- International Personal Data Transfer
Description	The Data Controller MUST provide information in the event of a personal data transfer to third countries or international organizations, taking into account that a transfer to a third country or an international organization may only take place under the circumstances defined in the GDPR.

4.2.3. Core principle to ensure data protection compliance – no processing of personal data within LIGHTest infrastructure or through the DNS for the duration of LIGHTest

The sections above have summarised the main requirements in relation to the processing of personal data under EU data protection law. However, within the context of the LIGHTest project the publication of personal data (or its subsequent translation or validation) into the DNS system is not required for any of the envisaged pilots or use cases. As described specifically in D3.2 - Conceptual Framework for Trust Schemes (2) and in D2.3 - Requirements

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

and Use Cases, the functional requirement of LIGHTest is for trust scheme information to be published, translated and validated. These actions in relation to trust schemes however do not require the processing of personal data. Therefore, **data protection compliance challenges cannot occur within LIGHTest in the context of the use of DNS.**

As explained in greater detail in D1.2, this does not imply that no personal data processing can occur *in relation to* the LIGHTest project. To the contrary, it is clear and certain that personal data processing will often occur *before or after* the use of LIGHTest infrastructure.

By way of a practical example: the validation of a signature will typically require the processing of personal data in order to determine whether the signatory is who they claim to be. However, this is a form of data processing that will occur outside the context of the LIGHTest infrastructure: LIGHTest will be used to discover trust policies in relation to which types of signatures are considered trustworthy by a relying party (e.g. whether signature solutions issued in country A are legally equivalent to those accepted in country B). However, this transaction does not require the processing of personal data of the signatory within LIGHTest: LIGHTest is only involved in the publication, translation and validation of trust policies, not in any subsequent processing of personal data. By way of comparison: the European Commission and Member States publish trust lists[3] that contain the same information that LIGHTest aims to make accessible via DNS; this publication of trust lists does not imply any processing of personal data, even if relying parties use this information to validate European signatures, as indeed occurs in practice[4].

In such cases, the LIGHTest infrastructure is a tool that may enable personal data processing outside the infrastructure and outside the context of the LIGHTest project, rather than as an inherent part of it. While it would in theory be possible to publish personal data into the DNS using LIGHTest tools, upon analysis the LIGHTest consortium cannot conceive of a use case where this would be required to enable the desired functionality. Provided that this observation proves to remain correct as the project continues, any publication of personal data in the DNS would be contrary to EU data protection law, as it violates the principles of lawfulness and data minimisation: if the publication of personal data is not *required* for the purposes envisaged by a specific use case, then the publication (or any subsequent processing) can be neither lawful nor in accordance with the data minimisation principle. Therefore, **LIGHTest takes the clear**

[3] See https://ec.europa.eu/digital-single-market/en/eu-trusted-lists-trust-service-providers

[4] By way of example: the Adobe Approved Trust List integrates and references the European national trust lists, thus allowing relying parties to validate European signatures via the Adobe PDF Reader. See https://ec.europa.eu/digital-single-market/en/eu-trusted-lists-trust-service-providers. This does not imply any transfer of personal data by the European Commission or any Member State to Adobe.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

position that personal data will not be published into the DNS in the context of the LIGHTest project, thus mitigating data protection compliance issues.

None the less, LIGHTest does not consider such incidental processing to be irrelevant. For this reason, the privacy by design principle of the GDPR[5] has been followed by: (i) implementing proper security measures within the infrastructure and (ii) providing guidance on LIGHTest data protection impact assessments (see directly below) that can be applied to any use cases – both inside of LIGHTest and after its completion - that will use the LIGHTest infrastructure. This framework can be used both for the LIGHTest pilots themselves and for any use cases outside the LIGHTest context.

4.2.4. The importance of data protection impact assessments

Within LIGHTest, legal data protection compliance requirements are principally addressed by abstaining from any processing of personal data to NEC using LIGHTest infrastructure. This is a perfectly viable approach within the context of LIGHTest as a project in which specific use cases will be piloted between a controllable and verifiable group of participants.

However, the consortium is aware that, after the termination of LIGHTest or beyond its own activities, the outputs of the project may be used by third parties for whom this approach is less intuitively obvious. Furthermore, use cases will very frequently involve data processing prior or after using LIGHTest infrastructure, as explained above. In those cases too, it is ethically required to ensure that guidance on the proper use of LIGHTest is made available, so that the practices adopted by LIGHTest – notably the requirement not to process personal data via DNS – are adopted elsewhere as well, and more broadly to ensure that any data protection risks and mitigation measures are identified correctly. This is necessary to ensure that LIGHTest is not inadvertently used for purposes that harm EU data protection requirements.

For this reason, **it is strongly recommended to conduct formal data protection impact assessments (DPIAs) whenever the LIGHTest technology is applied in a use case involving personal data.** In the sections below, we will briefly examine the concept and core requirements for DPIAs; identify useful resources which have been applied during LIGHTest; and highlight particular points of attention when using LIGHTest.

[5] ENISA, “Privacy and Data Protection by Design”, January 2015, https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 737460

4.2.4.1. Data protection impact assessments under EU law

Data Protection Impact Assessments (DPIAs) are a risk management and compliance instrument that have been given a specific legal basis under EU data protection law via the GDPR. Specifically, Article 35.1 of the GDPR requires a DPIA to be conducted where "a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons […]". Given the potential breadth of the processing activities in LIGHTest (or rather, the breadth of the processing activities which can be conducted using the LIGHTest architecture, including after the conclusion of LIGHTest), a DPIA is appropriate as a tool to identify and mitigate data protection risks.

The GDPR requires that DPIAs are conducted prior to the processing, i.e. before applying LIGHTest technology to a real-life use case involving personal data, consistent with data protection by design and by default principles (as indicated in section 4.2.2.). As a tool for helping decision-making concerning the processing, it is beneficial to conduct a DPIA as early as possible in order to be able to identify and implement mitigating measures. Moreover, DPIAs should be updated throughout the project lifecycle, in order to ensure that data protection and privacy are considered continuously, and that newly emerging issues can be addressed and resolved appropriately. Carrying out a DPIA is a continual process, not a one-time exercise.

The methodology of a DPIA is determined by the requirements of the GDPR, as interpreted and commented by the Article 29 Working Party's Guidelines on Data Protection Impact Assessments[6]. As the Guidelines indicate, a DPIA is a process designed to describe the processing, assess its necessity and proportionality and help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data by assessing them and determining the measures to address them. DPIAs are important tools for accountability, as they help data controllers not only to comply with requirements of the GDPR, but also to prove that appropriate measures have been taken to ensure compliance with the Regulation. In other words, a DPIA is a process for building and demonstrating compliance (although conducting a DPIA alone is of course not sufficient to ensure compliance; the broader

[6] Guidelines on Data Protection Impact Assessment (DPIA) (wp248rev.01), as last revised and adopted on 4 October 2017; see https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

legal, ethical and societal assessment framework in Section 5 will help to identify and address other compliance priorities).

Methodologically, DPIAs should at a minimum contain:

- a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;
- an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
- an assessment of the risks to the rights and freedoms of data subjects; and
- the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the GDPR, taking into account the rights and legitimate interests of data subjects and other persons concerned.

While some of these topics are partially common to all LIGHTest use cases – insofar as some risks and mitigation measures are defined by the LIGHTest architecture - the context of individual use cases is the key factor in determining risks and impacts on data subjects. For this reason, a DPIA must be conducted at the level of use cases, not on the project as a whole; the latter would be too generic and abstract to permit a reasonable DPIA to be completed, given that potentially any kind of personal data might be processed via the architecture.

Furthermore, it is important to stress that a DPIA is a formal exercise, that should result in a written report, as a part of the accountability duty incumbent on the data controller – i.e. the report will help the data controller to demonstrate that they have taken their compliance burden seriously.

In the sections below, we explain how a DPIA should be conducted, followed by particular points of attention when using LIGHTest infrastructure.

4.2.4.2. Key resources for DPIAs

The GDPR does not prescribe any particular methodologies for conducting a DPIA. Data controllers are therefore permitted to choose any framework which complements their existing working practices, provided that they contain the mandatory elements mentioned above. This flexibility allows them to select an approach that meets any national or sectorial best practices which are available to them, or to create a bespoke approach that aligns with their individual risk management approach.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

Within the LIGHTest use case, we have applied the methodology and structure of the international standard ISO/IEC 29134:2017 - Information technology -- Security techniques -- Guidelines for privacy impact assessment[7]. This standard was useful in particular for providing not only a clear structure (i.e. a table of content for the DPIA), but also a predefined classification of risk sources and threats.

As a software tool for modelling the DPIA, use was made of the open source software made freely available by the French data protection authority CNIL[8]. This facilitated completeness of the DPIA and ensured that the approach was aligned with the expectation of one of Europe's leading authorities.

The findings were thereafter extracted from the software into a written report. A sample report is attached as Annex I to this deliverable.

4.2.4.3. Particular points of attention when conducting DPIAs using LIGHTest technology

The LIGHTest experience has shown that DPIAs are an effective method for evaluating risks and identifying appropriate mitigation measures. In the context of LIGHTest's technology, there are several aspects that create particular complexities which should be examined in greater detail in any DPIA. These are described in the following sections. It is strongly recommended to address these issues explicitly and with particular focus in DPIAs using LIGHTest technology (as has also been done in the sample DPIA in Annex I).

No personal data in the DNS

The principal point of attention relates to the core principle stated above: LIGHTest experience has shown no cases where it is required to publish personal data directly into the DNS. This statement relates both to directly identifiable information (such as names, publicly available contact information, addresses etc.) and to indirectly identifiable information (such as identification numbers, unique job titles, private contact information etc.). Therefore, following the principle of data minimisation, such publication should not be engaged in, as it creates a

[7] Available at https://www.iso.org/standard/62289.html
[8] Available at https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

vector of abuse of personal data – by facilitating its collection and uncontrolled further use - which can be avoided.

This statement may seem at odds with one of LIGHTest's use cases, namely permitting delegations. However, while it is indeed possible to publish delegation information directly into the DNS system (e.g. indicating who is legally permitted to represent a specific company controlling a certain domain name), it is equally possible to only publish references in the DNS to a resource table containing this data. In that way, data publication on the DNS can be minimized, and control over the data can be optimised since the accessibility of the resource table can be controlled through authorisation management (unlike for DNS). It is therefore recommended to apply this control, rather than publishing personal data directly onto the DNS.

Thus, **a DPIA should assess whether the data minimisation principle has been applied by avoiding personal data publication, or justify why publication was lawful, proportionate and necessary for that particular use case.**

Multitude of LIGHTest roles and data sharing

As described in D2.6 - Formal Description and Analysis of Concepts (3), LIGHTest foresees a multitude of different functions and roles, which may or may not be relevant to a particular use case. Principally, these roles relate to the publication of trust schemes, translation of trust, and delegation – and of course the validation of specific transactions. While most LIGHTest use cases involve at least publication and validation, translation and delegation will be less common in practice.

Any role requires a specific authority to take action – e.g. by publishing a trust scheme, by verifying a translation, by managing delegation information, by validation transactions, and so forth. These roles can in practice be assigned to a single organisation, or they may be split between multiple organisations (with e.g. one organisation publishing a trust scheme, and another being in charge of translation to other trust schemes).

It is important for a DPIA to assess which of these roles will be relevant, who will take charge of each role, and whether any personal data exchanges between organisations will occur as a result of the role allocation. Data exchanges between organisations will require written arrangements to be established, governing the distribution of responsibilities and permissible use of the personal data.

Data minimisation and pseudonymisation

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

The section above already commented on the fact that personal data should not be published directly into the DNS. However, data minimisation is a general principle of the GDPR – personal data must be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed" (article 5.1 c of the GDPR, as also commented in section 4.2.2 above).

This implies that, when personal data is not processed via the DNS but rather via external resources – such as databases – which can be discovered via LIGHTest references, the data which is made accessible in those databases should be minimised as well, including by pseudonymising it wherever possible, in order to avoid needless exposure.

By way of example, if LIGHTest is used to discover the representatives of a specific organisation by pointing to a database of members of that organisation (including names, titles, and contact information), care should be taken that this database contains only the members who are actually representatives (and not all personnel members), and that this database only exposes the information which is actually required (and not all available personal data). Otherwise, even if LIGHTest is not the cause of the data protection compliance problem, LIGHTest none the less augments the risk that was already taken by needlessly exposing personal data to use and abuse.

Thus, **a DPIA should examine exactly whether data has been minimised appropriately, and whether LIGHTest risks creating new exposure to abuse.** If so, mitigation measures should be taken wherever possible.

Transparency and information notices

One of the key requirements of the GDPR is that the persons concerned must be informed of the data processing related to them, including the identification and contact data of the responsible entities (data controllers), the purposes of processing, recipients of data, and data retention (article 13 of the GDPR). A particular challenge when applying this principle to LIGHTest is that it generally is not used as a standalone form of data processing with its own unique purpose. Rather, LIGHTest is a supporting technology which is used as an infrastructural solution for a broader use case. This complicates transparency, as is always the case with supporting technologies: when using e.g. mobile banking, the bank will provide information on its mobile app, but likely not on the underlying database management systems, communication protocols, security technologies etc., even when these are provided by third parties. The same applies to LIGHTest.

This issue is also very context dependent. When LIGHTest is indeed purely used by a service provider who operates its own LIGHTest infrastructure under its own control, without any data sharing towards third parties and without triggering any new usage of the personal data,

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

additional information need not be provided to the end users, and LIGHTest usage can remain entirely invisible. When external LIGHTest authorities are used – e.g. an external LIGHTest delegation information provider – then exchanges of personal data do occur which must be notified to the data subjects.

For a DPIA, this implies that **the report should clearly indicate whether external parties are relied upon, and whether additional information provision to data subjects is required under the GDPR.**

Security, logging and auditability

The GDPR requires in general terms that any processing of personal data requires the implementation of appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with the GDPR. Those measures must be reviewed and updated where necessary (article 24.1 of the GDPR).

When deploying LIGHTest technology, this implies (among other obligations) that logging measures are enabled that allow individual transactions to be reconstructed, at least in use cases where legal challenges can occur. This is particularly necessary when LIGHTest is used to engage in legally relevant transactions, such as the sending of formal notification messages that can trigger the initiation of legal deadlines (e.g. notices of termination of an agreement), or the conclusion of contracts. In these cases, log files are a critical tool to determine whether a transaction has indeed taken place, and to determine whether they were completed correctly.

In LIGHTest, such logging is enabled by default (following the privacy by design principle), but care must be taken that logs are accessible to the parties that rely on them. This is a functional issue that cannot be standardised, since in some cases logs may be freely accessible, whereas in others they must be stringently protected.

A DPIA should therefore reveal which logs are available, and under what circumstances (and to whom) they are available for auditing.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

4.3 The eIDAS Regulation and its impact on LIGHTest

4.3.1. eIDAS as a driver behind LIGHTest

As described in the introduction, the eIDAS Regulation was to some extent a trigger for the entire LIGHTest project, as one of its core objectives is to support its application in practice. The Social Impacts Report (D2.9) described this background in detail, noting that within the EU, the eIDAS Regulation governs electronic identification and trust services by regulating:

- The cross-border recognition of specific means of **electronic identification**. Essentially, the eIDAS Regulation allows Member States to notify means of electronic identification (such as eID cards or mobile identification systems) which are used towards the public sector within their own borders, and, subject to certain legal requirements and procedures, thereafter requires other Member States to recognise these notified means within their own e-government applications as equivalent to their own national means of electronic identification.
- The legal value of certain well-defined **trust services,** specifically electronic signatures, electronic seals, time stamps, electronic registered delivery services, and website authentication. Contrary to the provisions on electronic identification (which are oriented towards the public sector), the provisions on trust services emphatically consider these as market services which can be provided and used in a purely public sector context.

Given the scope of the eIDAS Regulation, it provides a clear legal underpinning for answering some of the most crucial trust management questions, including who a person is and who they represent (both covered under electronic identification), whether a communication comes from them and whether it has been changed (provided by electronic signatures and electronic seals), when a specific piece of information existed (time stamps), whether a website is controlled by the entity claiming control over it (website authentication), and whether a message was securely sent and received by specific identified entities (electronic registered delivery services).

In order to make sure that the Regulation functions effectively and that these services can all be deployed in the market, the Regulation establishes a very clear trust management framework in relation to these services. Specifically:

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

- Means of electronic identification, once they are notified by a Member State, undergo a peer review process by other Member States which takes one year, culminating in the publication of the means of electronic identification in the Official Journal (Article 9).
- The most trustworthy[9] trust service providers (referred to as qualified trust service providers in the Regulation) are required to undergo biannual external audits, the result of which must be presented to supervisory authorities which are designated in each Member State. Provided that the audit results are accepted, the providers are thereafter listed in a so-called trusted list, published by the supervisory authority in a standardised EU level format (Article 22).

Electronic identification and trust services under the eIDAS Regulation thus have a relatively clear trust management model behind them: a third party can rely on notified identities and qualified trust services because their assurances are legally defined, independently audited, and the outcomes are made public via the Official Journal (for identities) and national trust lists (for trust services). The published trust information is therefore available to support trust decisions.

LIGHTest aims to implement the exact same trust model behind eIDAS using the DNS system. The trust model remains intact: electronic identities would still be notified and assessed as eIDAS requires, and qualified trust services would still be audited and supervised by national supervisory bodies. But rather than publishing the outcome only in the strictly European Official Journal and trust lists, the outcome would be published in the DNS as well. This would still allow third parties to access and validate the information, since only the medium of communication of the trust information changes. More importantly, other regions of the world could easily follow suit by publishing their own trust information (e.g. in relation to trusted identities in China, or trust services in the USA) in the DNS system, creating interoperability without having to adhere to a European ruleset or standard.

[9] More accurately, this obligation is incumbent only on so-called qualified trust service providers, which must satisfy harmonised requirements in the Regulation. Nonqualified trust service providers can in principle offer equal or ever higher quality services, but as they are not necessarily assessed by a third party on this point and as they are not *ex ante* supervised by national supervisory bodies either, it is up to customers to verify on a case by case basis whether they consider a nonqualified trust service provider to be suitable for their purposes. It is not obligatory for a trust service provider to become qualified; this is a market decision that the trust service provider can make, by considering whether the cost and effort of being qualified (notably the expenses of the recurring audits) are offset by the market opportunities of being qualified.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

4.3.2. eIDAS compliance requirements in LIGHTest

When examining eIDAS compliance requirements in LIGHTest, it is worth repeating that LIGHTest does not change the trust model behind eIDAS (and in fact, relies upon it). Furthermore, LIGHTest does not affect substantive rules in relation to electronic identification or trust services: it does not affect which eIDs can be notified, what the relevant procedures are, or how they are approved or rejected; nor does it change the definition of qualified trust services, their legal value, or interoperability and liability rules.

LIGHTest does however affect the publication, validation and translation of trust information. Within eIDAS, this could conceptually pertain notably to the following:

- The publication at EU level of notified means of electronic identification in the Official Journal (Article 9.2);
- The publication at Member State level of trusted lists containing at least the qualified trust service providers which are supervised in that Member State (Article 22.1);
- The publication at Member State level of lists of national conformity assessment bodies (CABs), which are accredited for carrying out conformity assessments of qualified trust service providers and the qualified trust services they provide (Article 3.18 of eIDAS; the accreditation process as such is governed by Article 2 of Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC));
- The publication at Member State and EU level of lists of certified qualified signature/seal creation devices that can be used to create qualified signatures/seals (Article 31).

For all of the obligations above, eIDAS requires trust information to be published in a way that enables its validation. Implementing such lists via the DNS instead would be viable in each of the four cases. In practice however, LIGHTest presently envisages to only pilot the publication and validation via the DNS of the trusted lists containing at least the qualified trust service providers (Article 22.1), and not the other three types of trust information under eIDAS.

The reason for this focus is practical: the trusted lists of Article 22.1 must be published using a technical specification that has been standardised and harmonised, namely the European

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

technical specification (ETSI TS 119 612), which must mandatorily be used under an implementing decision of the eIDAS Regulation[10]. Furthermore, links to the national trust lists are published on a website of the European Commission, making the national information easy to find and integrate in an exhaustive manner.

In contrast, the other three categories of information all have availability issues. A small number of eIDs have undergone a full notification process at the time of writing of this deliverable[11], but the relevant information is published only in a human readable form – not in a structured machine readable form that would be suitable for direct integration into the DNS Information on approved CABs and certified devices is available from some countries, but not systematically, and not in a harmonised format. Given the lack of standardisation, this information is harder to integrate into the DNS without creating fidelity issues (i.e. without creating the risk that third parties challenge the accuracy or value of the information in LIGHTest on the grounds that it is not identical to the information published at the national level).

Therefore, the national lists of qualified trust service providers are the main source of information to be integrated into the DNS.

As noted above, LIGHTest relates to the publication and validation of trust information (covered by the publication of trust list information in the DNS and enabling its use in trust service use cases), but also to trust translation. Trust translation essentially relates to an assessment and finding of equivalence between specific trust schemes. In practical terms, under the eIDAS Regulation trust translation can refer to:

- Equivalence between European means of electronic identification and non-European ones;
- Equivalence between European qualified trust service providers and non-European trust service providers (which would not be called ‘qualified’, since this is a European concept).

The eIDAS Regulation in fact foresees mechanisms to support trust translation from a legal perspective: Article 14 allows trust services provided by trust service providers established in a third country to be recognised as legally equivalent to qualified trust services provided by

[10] Specifically Commission Implementing Decision (EU) 2015/1505 of 8 September 2015 laying down technical specifications and formats relating to trusted lists pursuant to Article 22(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

[11] See the Overview of pre-notified and notified eID schemes under eIDAS; available at https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 737460

qualified trust service providers established in the Union, provided that such third country trust services originating from the third country are recognised under an agreement concluded between the Union and the third country or an international organisation. No equivalent rule exists in relation to electronic identification.

In practical terms, this means that trust translation will mainly relate to trust services. At the time of drafting of this deliverable, no such agreement is in place yet, and therefore no non-European trust services are legally recognised as being equivalent to European qualified trust services yet. Therefore, any piloting on this point will either be limited to a proof-of-concept only without binding legal value, or be limited to a specific context in which a given party voluntarily accepts the equivalence of a non-European trust service, despite the lack of any legislative basis for this decision (i.e. a party would accept the risk of making this decision by itself, on the basis of its own appreciation of its legal needs and available assurances).

In summary, the legal requirements linked to the eIDAS Regulation relate mainly to the accurate translation of the trust information from national trusted lists as governed by the eIDAS Regulation, and to the clear communication that other legal assurances must be provided externally: LIGHTest will not affect (positively or negatively) the legal value or validity of electronic identification, trust services, or trust translation, and this position must be clearly communicated to relying parties. Summarising it using the template above, this can be captured as follows:

No.	eIDAS-1.00 - Accurate Trust List Integration
Description	Supervision information in relation to qualified trust service providers within LIGHTest MUST be sourced directly from national trusted lists as governed by Article 22 of the eIDAS Regulation.

No.	eIDAS-2.00 – Direct Application of eIDAS Regulation
Description	In any pilot cases, the service provider MUST make clear that the use of LIGHTest does not imply legal assurances beyond those which are provided under applicable law (including particularly the eIDAS Regulation) or by the service provider on a contractual basis. Use of LIGHTest as such does not provide any additional legal guarantees or assurances.

No.	eIDAS-3.00 – Transparency on Legal Framework
Description	In any pilot cases, the service provider MUST make clear to relying parties that the source of trust information is the trusted lists themselves, and that LIGHTest merely serves to make this information available in an unmodified form.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

No.	eIDAS-4.00 – Trust Translation Decisions
Description	LIGHTest cannot provide legal assurances on the value or validity of translation of trust schemes while no agreements covered by the eIDAS Regulation have been concluded between the Union and third countries. Any trust translation information provided by LIGHTest MUST therefore be subject to a decision of the relying party itself on the acceptability of the trust translation for its own purposes.

No.	eIDAS-5.00 – Assurances from the Service Provider
Description	LIGHTest is a technology that can be used to communicate, validate or translate trust schemes, but which has no built-in assurances other than requirement eIDAS-1.00, i.e. the fact that trust information on qualified trust service providers originates from official national level trusted lists. Therefore, a service provider using LIGHTest technology MUST communicate to the customer which legal assurances they provide and which liabilities they accept (if any) through contractual terms.

It is worth highlighting that the requirements above constitute the baseline of what LIGHTest technology can offer 'out of the box', i.e. without a service provider building a service around it. In reality, service providers will use the LIGHTest technology to provide trust information services to their own constituency that extend beyond the basic requirements of the eIDAS Regulation. By way of a simple example: an electronic signature validation service that just supports the validation of qualified electronic signatures has limited added value from LIGHTest, since this is a functionality that is supported by the eIDAS trust lists 'out of the box', without third party support.

However, LIGHTest's added value is flexibility. This becomes visible when the service provider not only offers validation of qualified electronic signatures, but also of a range of non-qualified electronic signatures (which by definition are not included on the European trusted lists). This kind of validation functionality which is absent from eIDAS can easily be incorporated using LIGHTest's tools, and requires the service provider to make the necessary risk assessments and define its own commercial terms (i.e. the service provider must decide itself what kind of assurances of equivalence it provides to its customers and what kind of liabilities it offers).

This dependence on the service provider's own business decisions and the need to define contractual terms is reflected in requirement eIDAS5.00 above, indicating that service providers using LIGHTest technologies must contractually delineate their responsibilities and liabilities. This reliance on contractual terms is inevitable when a project delivers a technology that can be applied in a wide range of use cases, rather than one single use case.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

As was already highlighted earlier however, LIGHTest does provide assistance in the creation of such contractual frameworks: sample contractual terms and conditions have been made available in:

- D3.7 - Cross-Border Legal Compliance and Validity of Trust Scheme Publication - containing sample contractual terms for trust scheme validation;
- D4.7 - Cross-Border Legal Compliance and Validity of Trust Scheme Translation - containing sample contractual terms for trust scheme translation;
- D5.7 - Cross-Border Legal Compliance and Validity of Delegation - containing sample contractual terms for delegation.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

5. Defining a legal, ethical and societal assessment framework for LIGHTest

5.1 Introduction

The sections above have illustrated how LIGHTest handles data protection compliance and eIDAS compliance, as the two principal legal frameworks at the EU level that govern the use cases in LIGHTest. However, the consortium is aware that, after the termination of LIGHTest or beyond its own activities, the outputs of the project may be used by third parties who have other use cases in mind, which may not involve personal data, or which may not involve any electronic identification or trust services as contemplated in eIDAS. In those cases too, guidance should be available on the proper use of LIGHTest and on the identification and resolution of legal, ethical and societal issues.

For that reason, as briefly described above, LIGHTest has defined an assessment framework for any use cases of the LIGHTest infrastructure. This assessment framework – which can be combined with a formal data protection impact assessment as may be required under the GDPR - provides guidance on available options to ensure compliance with legal, ethical and societal requirements.

There are many applications of the LIGHTest technology which do not involve the processing of personal data, nor the use of trust services. Deliverable D2.3 - Requirements and Use Cases explored some of these in detail, but by way of a simple example: a European trade association could use LIGHTest to publish a list of its member companies and their categories of activities, thus allowing relying parties (consumers, companies and public authorities alike) to find and validate this information easily. In an international context, an international trade association could even use LIGHTest to link to European, American and Chinese trade associations, who in turn use LIGHTest to publish their members. In this way, LIGHTest is used for publication and validation of trust information by the regional trade association (who identify their respective trusted members), and for trust translation by the international trade association (who identifies the trusted regional trade associations). In these cases, neither data protection law nor eIDAS are relevant.

Since the number of application areas is practically unlimited – LIGHTest can be used whenever trusted information must be published, validated or translated – it is also not possible to abstractly list out all possible legal requirements. To continue the example above: while the trade associations may not need to worry about data protection or eIDAS, they will need to

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

ensure that the members respect their internal rules, and that suspended members are removed from the list. Furthermore, membership might be dependent on the members meeting sector specific legal requirements on quality, protection of health and safety, or national audits and supervision. In other words, one cannot draw up a detailed yet abstract list of requirements that would apply in all cases.

However, it is possible to define an analytical framework that allows legal, ethical and societal challenges for LIGHTest use cases to be identified. In this Chapter, we will create such an assessment framework, which can thereafter be applied to any LIGHTest use cases (including those that will be piloted in LIGHTest, but also any LIGHTest use cases that would be implemented outside the confines of the project), in order to identify and address their specific legal, ethical and societal challenges.

The framework should consist of a statement of principles that can be used as assessment criteria to determine whether any LIGHTest use case is likely to encounter specific types of legal, ethical and societal challenges and what the resulting requirements might be. The logical structure therefore looks as follows:

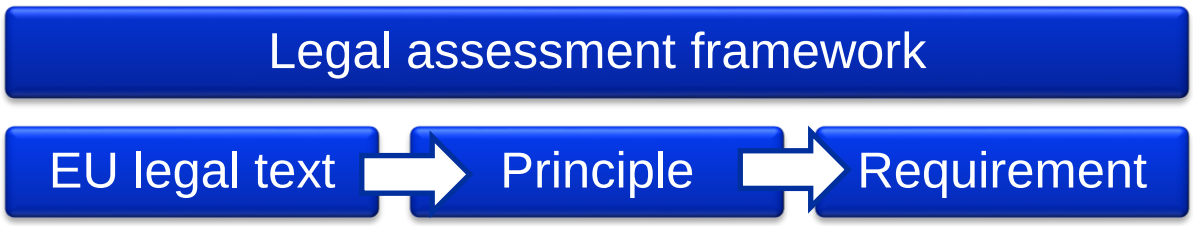

Figure 1: Legal, ethical and societal assessment framework: an EU legal text is the source of a principle, which defines requirements

Given this scoping, the following principles apply to the legal, ethical and societal assessment framework:

- The assessment framework, including the principles and the resulting requirements, must be **generic**, in the sense that it must be possible to apply the framework to any LIGHTest use case. No sector or context specific principles or requirements will be defined.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

- The assessment framework must be defined at the **European** level. This means that only EU level sources are used to define principles and requirements, excluding international, national or regional sources.
- The assessment framework must result in **requirements**: it is not a collection of source material and abstract principles, but must contain specific requirements that can be applied to LIGHTest use cases.
- The assessment framework must be **testable**, meaning that it must be possible to apply each of the requirements to a LIGHTest use case and to determine whether it has been complied with.

Methodologically, the assessment framework will be created by evaluating relevant EU level legal texts that meet the requirements of being generic – i.e. without going into the legislation governing individual use cases or specific pilot contexts – and attempting to extract or derive general legal, ethical or societal principles that will need to be adhered to when applying the LIGHTest technologies. Multiple texts can obviously support the same principles and even result in the same requirements; i.e. while each requirement and principle can be traced to at least one source, some requirements and principles are supported by multiple sources.

5.2 Sources, selection logic and relevance to LIGHTest

As noted above, the assessment framework is based on EU level texts as a source. This implies that a first selection had to be made of texts that were considered as relevant. The selection process was conducted based on two factors:

- Firstly, data protection law and the eIDAS Regulation were considered, since these constituted the baseline for LIGHTest as a project.
- Secondly, inputs from project partners were taken into account, since they are most likely to be intimately familiar with key legal, ethical and societal requirements.

The outcome of this process was the following list of source documents used, with the justifications indicated below.

Source	Justification for its selection

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

EU Charter of Fundamental Rights and the Universal Declaration of Human Rights	While generic, the Charter states the fundamental rights that should be observed by the institutions and bodies of the EU, and by national authorities only when they are implementing EU law. It includes testable rights that are critical to the correct application of LIGHTest, such as the right to good administration (including transparency and impartiality), the right to justice (right to appeal and the right to be heard), and the right to privacy / data protection. The Universal Declaration of Human Rights was additionally screened to solidify international usability of the framework.
Data Protection Directive (DPD), General Data Protection Regulation (GDPR) and the APEC Privacy Framework	The right to data protection is a fundamental right as indicated in the Charter, and implies that any LIGHTest use case where personal data is processed will need to adhere to applicable data protection law. Until 25 May 2018, the DPD (or rather its national transpositions) applies; thereafter the national data protection laws will largely be supplanted by the GDPR. The APEC Privacy Framework was additionally screened to solidify international usability of the framework.
eIDAS Regulation and the UNCITRAL Model Law on Electronic Signatures	The eIDAS Regulation provides a homogeneous legal framework for electronic identification and certain trust services across the EU. The identification of citizens and businesses will be critical to the successful implementation of LIGHTest. The UNCITRAL Model Law on Electronic Signatures was additionally screened to solidify international usability of the framework.
Services Directive	The Services Directive aims to support the free movement of services in the internal market by removing legal and administrative barriers to trade for the services within its scope. While it does not govern LIGHTest as such, it contains administrative simplification obligations and implementation measures (such as the creation of national Points of Single Contact) that aim to ensure that service providers can easily exchange trustworthy electronic information from one Member State to the next.
e-Commerce Directive, the UNCITRAL Model Law on Electronic Commerce, and the United Nations Convention on the Use of Electronic Communications in International Contracts.	The e-Commerce Directive is relevant to many conceivable LIGHTest use cases, since it defines a series of legal principles in online interactions, including with respect to the validity of electronic transactions, information and transparency requirements, liability and dispute settlement in cross border contexts. The UNCITRAL Model Law on Electronic Commerce and the United Nations Convention on the Use of Electronic Communications in International Contracts were additionally screened to solidify international usability of the framework.

Table 1: Legal source documents for the legal assessment framework

While not comprehensive, this regulatory package was selected in order to identify relevant legal, ethical and societal principles for LIGHTest use cases. The GDPR has been taken into account as of the beginning of LIGHTest, even though it only became applicable on 25 May 2018, due to its practical importance to LIGHTest and the European information economy.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

5.3 Principles of the assessment framework and resulting requirements

Based on an analysis of the aforementioned sources, the following visual canvas containing the principles of the assessment framework can be provided:

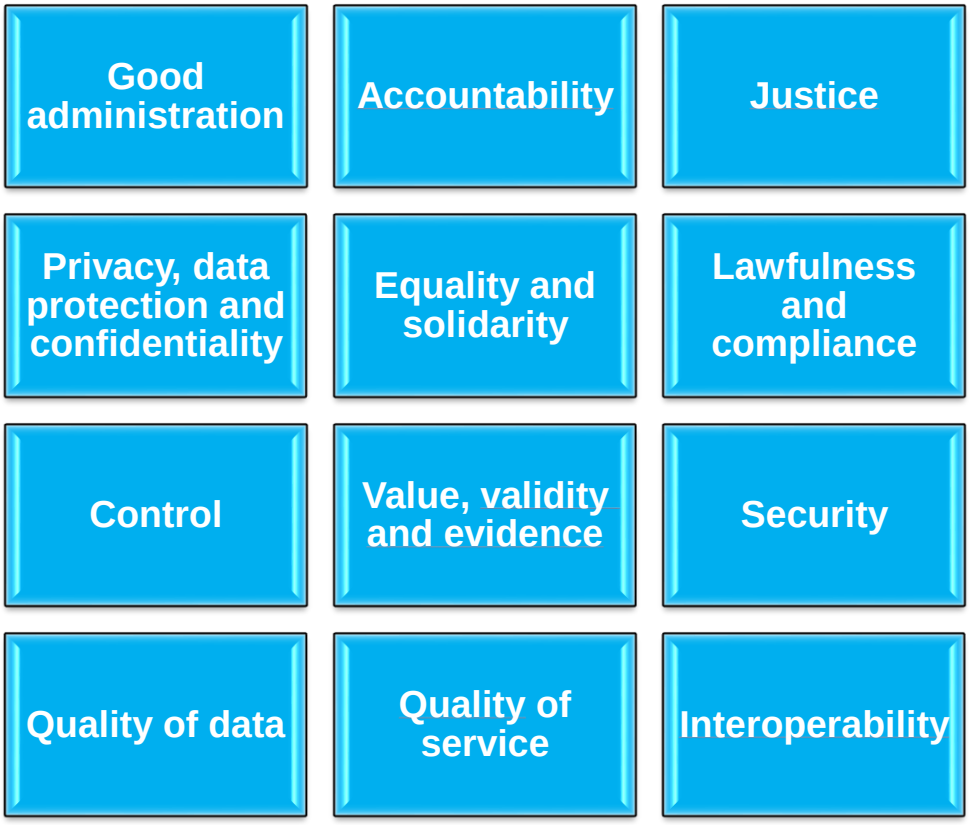

Figure 2: Canvas of the assessment framework

The canvas above only provides a summary statement of the principles. The table below provides a more detailed description of what each principle means, and what the resulting legal, ethical and societal requirements are. From a practical perspective, the table can be

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

considered as a legal checklist to be applied to each LIGHTest use case, allowing a determination of whether legal, ethical and societal requirements have been satisfied. It should be noted that it is always somewhat arbitrary to decide whether a given principle should indeed be considered as separate or as a sub element of another principle; it could for example be argued with some merit that the principle of accountability is a subsection of the broader principle of good administration.

However, the key element is that the requirements are defined appropriately, since these will be the criteria through which any LIGHTest use case will be tested. The importance of the demarcation of principles or the allocation of requirements to one principle or another should not be overestimated.

Principles	Description and resulting requirements
Good administration	**Description**: LIGHTest technology must be implemented in a way that ensures that transactions are handled impartially, fairly and within a reasonable time. **Requirements**: • LIGHTest technology must be implemented in a way that ensures non-discrimination: trust information must be transferred on a neutral basis, without prejudicing any decisions that would be made by the receiving party on the basis of the trust information. • LIGHTest technology must be implemented in a way that ensures transparency: the trust information to be transferred, its origins and meaning must be clearly known to the recipients. • LIGHTest technology must be implemented in a way that facilitates comprehension: without prejudice to the autonomy of the receiving party to make any decisions on the basis of the information received, it must at least be able to semantically interpret the information.
Accountability	**Description**: LIGHTest technology must be implemented in a way that ensures that responsibilities are clearly allocated between each participant in the exchange of trust information. **Requirements**: • LIGHTest technology must be implemented in a way that ensures that all participants are aware of their obligations and responsibilities, and notably what assurances are provided behind the communicated trust information. • The persons relying on LIGHTest technology must have the right to restitution of any damages caused by noncompliance with these obligations insofar as this is possible under applicable law and the contractual terms of the entity using LIGHTest.
Justice	**Description**: LIGHTest technology must be implemented in a way that ensures the right to recourse for the persons relying on LIGHTest technology, and that contains appropriate enforcement mechanisms. **Requirements**:

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

	• LIGHTest technology must be implemented in a way that safeguards the right of every person to be heard, before any individual measure which would affect him or her adversely is taken on the basis of trust information exchanged via LIGHTest. • LIGHTest technology must therefore be implemented in a way that provides appropriate contact mechanisms for persons relying on LIGHTest as recipients or as relying parties on trust information communicated via LIGHTest.

Privacy, data protection and confidentiality	**Description**: LIGHTest technology must be implemented in a way that safeguards the fundamental rights to privacy and data protection for natural persons, and respecting the legitimate interests of confidentiality and of professional and business secrecy.
	Requirements:
	• LIGHTest technology should be implemented in a way that avoids the publication of personal data via the DNS, as explained in Chapter 3 of this report.
	• Any personal data processing in relation to the use of LIGHTest technology may only occur in accordance with applicable data protection law, notably the DPD, or as of 25 May 2018, the GDPR. This includes the principles of:
	  ○ lawfulness, fairness and transparency;
	  ○ purpose limitation;
	  ○ data minimisation;
	  ○ accuracy;
	  ○ storage limitation;
	  ○ integrity and confidentiality;
	  ○ accountability.
	• The requirements of Chapter 3 must at all times be adhered to.

Equality and solidarity	**Description**: LIGHTest technology must be implemented in a way that protects the persons concerned against discrimination. **Requirements**: • LIGHTest technology must be implemented in a way that ensures non-discrimination: trust information must be transferred on a neutral basis, without prejudicing any decisions that would be made by the receiving entity on the basis of the trust information. • LIGHTest technology must be implemented in a way that ensures universal accessibility, including to persons with disabilities. Accessible support and communication mechanisms must be provided to ensure that such persons can receive comparable functionality as any other persons benefiting from LIGHTest technology.
Lawfulness and compliance	**Description**: LIGHTest technology must be implemented in a way that ensures that trust information is only published, validated and interpreted in accordance with any specific legislation or other legal requirements that may apply to that trust information. **Requirements**: • Trust information may only be published, validated and interpreted through LIGHTest technology if it has been determined that any pre-existing legal requirements (including sector or context specific legal requirements) are satisfied,

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

	including national authorisation procedures, legal agreements on usage restrictions, assurances with respect to security, assurances or exclusions of liability, data or service quality arrangements, etc. The necessary contractual terms have to be implemented to ensure that these requirements are adhered to.
Control	**Description**: the implementation of LIGHTest technology must contain appropriate controls to ensure that the provided trust information is relevant and to allow incidents to be detected and addressed. **Requirements**: • Appropriate audit and logging measures must be implemented to ensure that any use of trust information which is made available via LIGHTest can be verified by competent authorities in case of disputes (including the identification of the sending and receiving parties, the time of the exchange, and the integrity/authenticity of the exchanged data itself).
Value, validity and evidence	**Description**: the legal value and validity of any trust information exchanged via LIGHTest must be clear to all participants in a transaction. **Requirements**: • There must be an agreement between service providers and relying parties on the legal value and validity of the trust information, including specifically whether it can be considered authoritative (as is e.g. the case for trust list information in relation to qualified trust service providers), or whether it can otherwise be relied upon to be genuine or to be covered by any contractual assurances.
Security	**Description**: LIGHTest technology must be implemented in a way that protects the exchanged trust information against modification during transit, thereby ensuring its integrity and authenticity to the extent required by the use case. **Requirements**: • Users of LIGHTest technology must follow LIGHTest's security measures and protect their infrastructure through appropriate technical and organisational measures to ensure a level of security appropriate to the risk. • Incident response measures must be implemented to ensure that the exchange of compromised trust information through LIGHTest is avoided, and can be notified to recipients if an incident should occur.
Quality of data	**Description**: LIGHTest technology must be implemented in a way that provides a clear shared understanding between all participants in the use case on the quality of the trust information. **Requirements**: • A legal framework must exist that clarifies the obligations of the participants in the use case in relation to the quality of the trust information, including any assurances of its accuracy, factual correctness, and timeliness of updates (which may take the form of legislation, SLAs, memoranda, or even nonbinding best efforts agreements; the requirement is that the understanding is clear).

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

	• A feedback mechanism must be in place that allows the persons involved to contact the entity at the source of the trust information to correct any inaccuracies.
Quality of service	**Description**: LIGHTest technology must be implemented in a way that provides a clear shared understanding between all participants in a use case on the quality of the services for the exchange of trust information. **Requirements**: • A legal framework must exist that clarifies the obligations of the participants in the use case in relation to the availability and responsiveness of the services (which may take the form of legislation, SLAs, memoranda, or even nonbinding best efforts agreements; the requirement is that the understanding is clear). • An evaluation mechanism must be in place that allows noncompliance with this framework to be detected and addressed when necessary.
Interoperability	**Description**: LIGHTest technology must be implemented in a way that ensures semantic and technical interoperability of the trust information exchanged via LIGHTest. **Requirements**: • Appropriate agreements must be in place with respect to the technical and semantic characteristics of the trust information, taking into account linguistic challenges and diversity of legal systems. Trust information should not be exchanged using LIGHTest if interoperability is not ensured.

Table 2: Assessment framework – principles and requirements

While this overview table is generic and designed to be applicable for all LIGHTest use cases, more specific and tailored versions have been created for each specific role – trust scheme publication, translation and delegation. These can be found in respectively D3.6, D4.6 and D5.6, along with sample contractual texts, allowing legal issues to be identified and resolved.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

6. Conclusions

This deliverable has provided a concise overview of how legal, ethical and societal requirements and constraints can be identified and dealt with when using the LIGHTest technology, from two perspectives:

- Firstly, the legal, ethical and societal challenges that relate directly to data protection law and the eIDAS Regulation have been identified and discussed in Chapter 4, since these are the central legal sources that drive compliance challenges in the pilot cases that the LIGHTest project aims to complete. General DPIA guidance is provided, along with an identification of DPIA attention points when using LIGHTest. A sample DPIA report for a LIGHTest use case is included in Annex I.
- Secondly, a broader and more generic assessment framework has been defined in Chapter 5 that consists of a statement of principles that should be respected in all LIGHTest use cases. While abstract, the assessment framework is intended to be used in practice as a systematic checklist to verify which legal, ethical and societal challenges are likely to occur, and therefore what assurances should be provided by the legal solutions created around a specific use case.

These outputs can be applied to the LIGHTest pilots and to any other use cases of LIGHTest technologies in order to ensure that legal, ethical and societal challenges can be addressed appropriately.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

7. Annex I – DPIA for the Trustworthy Communication Services Pilot

7.1 Process under evaluation - nature of the processing activities and types of personal data

The Trustworthy Communication Services Pilot examines possible use cases for the integration of Correos products with LIGHTest. It includes two scenarios[12]:

- "My Mailbox" ("*Mi Buzón*") is a digital service for citizens, companies and governments enabling them to send and receive documentation. Sender and receiver are validated and uniquely identified by Correos. Individuals subscribe to any verified business/government agency to start receiving trusted information. By means of LIGHTest, Correos service will validate that the entity sending a document operates under a known Trusted Scheme (eIDAS, NIST, etc.); querying, through the ATV, first to the TSPA to fetch the metadata of the Trusted Scheme claimed and check if it enables the sender, and second if it is necessary to query TTA to look for an equivalent trust scheme which enables the sender. Moreover, LIGHTest ATV would be used to inform users about document eDelivery LoA, and possible LoA translation in the case of non-national companies.
- "My Notifications" ("*Mis Notificaciones*") is a digital service foreseeing centralization and management of governmental eNotifications for one or several individuals or legal entities. In such secured and trusted communications, LIGHTest would be useful to offer value by double-checking with a certified entity in Europe that such communication is done accordingly to current legislation.

The **personal data processed** for this pilot is limited to what is strictly necessary, in accordance with the data minimisation principle. It relates notably to:

- Names of the persons involved in the communication
- Contact information of the persons involved in the communication
- Authentication information of the persons involved in the communication

[12] Described in more detail in D9.1 - eCorreos: Requirements, Scenarios and Demo Data; and in D9.4 Correos: LIGHTest Setup

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

- Correos customer identifiers of the persons involved in the communication

However, it is worth noting that this information is not processed (published, translated, validated or otherwise) through LIGHTest infrastructure. LIGHTest software will only be used to process datasets that will be necessary for each component of LIGHTest:

- DNS entries in the TSPA (as trust lists that includes the issuers for the stated scheme).
- Translation entries in the TTA for cross-border LoA translation.
- Trust Policies that can be automatically executed in the ATV (for all parties).
- ASiC packed transactions that can be given as input to the ATV (for all scenarios), including PKI infrastructure for the signing of the electronic transaction.

This is in accordance with the core principle of LIGHTest that no processing of personal data should occur within LIGHTest infrastructure or through the DNS for the duration of LIGHTest.

Furthermore, to correctly appreciate the risks, it should be considered that Correos already provides the aforementioned services in commercial applications with live data, without compliance issues. Thus, from a data protection perspective no new legal challenges should arise as a result of the use of LIGHTest tools.

The **legal basis** for the processing of personal data in the context of the Correos pilot can be found:

- In the **contractual relationship** which Correos has with its customers, acting as a data processor on their behalf;
- The **legitimate interests** of Correos for any processing that it undertakes separately from this contractual mandate in the organisation and participation in the LIGHTest project and its piloting activities. The legitimate interest is particularly justified considering:
    - The pilot scale of LIGHTest (i.e. the fact that risks and exposure are limited)
    - The expected benefit to the data subjects, both in terms of interoperability and in terms of privacy/security benefits

The elements above should be appropriate to ensure the lawfulness of processing with the context of LIGHTest.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

7.2 Risk criteria and privacy requirements

7.1.1. Risk assessment

7.1.1.1. Risk sources

Data protection risks include notably the following:

- unauthorized access to personal data (loss of confidentiality);
- unauthorized modification of the personal data (loss of integrity);
- loss, theft or unauthorized removal of the personal data (loss of availability);
- excessive collection of personal data (loss of operational control);
- unauthorized or inappropriate linking of personal data;
- insufficient information concerning the purpose for processing the personal data (lack of transparency);
- failure to consider the rights of the data subject (e.g. loss of the right of access);
- processing of personal data without the knowledge or consent of the data subject (unless such processing is provided for in the relevant legislation or regulation);
- sharing or re-purposing personal data with third parties without the consent of the data subject;
- unnecessarily prolonged retention of personal data.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

7.1.1.2. Threats within LIGHTest

The main threats from a data protection perspective relate to personal data and/or business information being inappropriately divulged, or misused for the purposes of identity theft, fraud or other criminal activities.

In all instances, leaving aside data protection harms, the unavailability of services can furthermore create substantive operational and economic harms – including delays in administrative proceedings and legal term limits expiring.

The following major threats can be identified, based on the Generic Threat listing of Annex B of ISO/IEC 29134:2017, as reviewed, filtered and amended on the basis of the pilot's general descriptions. It should be stressed that, since this DPIA targets the Correos pilot, threats relating to Correos' general data processing assets (i.e. its generic processing infrastructure which is not affected by LIGHTest) is not taken into account in this threat matrix. I.e. issues such as defects in Correos' hardware, network outages with a customer, data theft at Correos' side are not included in this matrix, since they are risks that exist outside the context of LIGHTest and are unaffected by it.

Supporting assets	Action	Privacy risk	Examples of threats
LIGHTest hardware	Overload, Loss or Damage	Disruption of processing	Storage unit full; power outage; processing capacity overload; overheating; excessive temperatures, etc.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

LIGHTest software	Abnormal use	Illegitimate accesses to the personal data	Content scanning; illegitimate cross-referencing of data; raising of privileges; wiping of usage tracks; sending of *spam* via an e-mail program; misuse of network functions, etc.
LIGHTest software	Abnormal use	Unwanted changes in the personal data	Unwanted modifications to data in databases; erasure of files required for software to run properly; operator errors that modify data, etc.
LIGHTest software	Damage	Disappearances of personal data	Erasure of a running executable or source codes; logic bomb, etc.
LIGHTest software	Modification	Disappearances of personal data	Errors during updates, configuration or maintenance; infection by malware; replacement of components, etc.
LIGHTest software	Modification	Illegitimate accesses to the personal data	Tracking by a software-based keylogger; infection by malware; installation of a remote administration tool; substitution of components, etc.
LIGHTest software	Modification	Unwanted changes in the personal data	Errors during updates, configuration or maintenance; infection by malware; replacement of components, etc.
LIGHTest software	Overload	Disappearances of personal data	Exceeding of database size; injection of data outside the normal range of values, etc.
LIGHTest computer channels	Overload or damage	Disruption of processing	Misuse of bandwidth; unauthorized downloading; loss of Internet connection, etc.
LIGHTest individuals	Abnormal use	Illegitimate accesses to the personal data	Influence (phishing, social engineering, bribery, etc.); pressure (blackmail, psychological harassment, etc.), etc.
LIGHTest individuals	Abnormal use	Unwanted changes in the personal data	Influence (rumour, disinformation, etc.), etc.
LIGHTest individuals	Espionage	Illegitimate accesses to the personal data	Unintentional disclosure of information while talking; use of listening devices to eavesdrop on meetings, etc.

Table 3: Threats

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

Thus, four threat vectors are considered under the LIGHTest project:

- **LIGHTest hardware**, to be understood as the hardware on which the LIGHTest connector runs. Unavailability of services is the most substantial risk here; data protection problems are limited to unavailability, since the messages exchanges by Correos are not stored in the LIGHTest infrastructure. Theft or loss of personal data, or inappropriate use, therefore cannot occur at the LIGHTest hardware level.
- **LIGHTest software**. The principal risks here are bugs, hacks, misconfigurations or modifications that cause corruption of data, removal of protections, interruption of data flows, or that affect access and usage rights.
- **LIGHTest computer channels**, to be understood as the network environment across which the LIGHTest components communicate, up to the point where the network falls under the control of the data consumer/provider. Here too the principal risk is unavailability of services, since Correos operates these channels itself. Theft or loss of personal data, or inappropriate use, therefore cannot occur at the LIGHTest computer channel level.
- **LIGHTest individuals** finally are those persons in charge of developing, installing, configuring or maintaining all of the vectors above (hardware, software, computer channels). The principal threats are the introduction of bugs, hacks, misconfigurations or modifications that cause corruption of data, removal of protections, interruption of data flows, or that affect access and usage rights (whether intentional or not).

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

7.1.1.3. Risk evaluation: likelihood of threats and their level of impact

The likelihood and impact of the aforementioned threats can be assessed using the standardised classification of Annex I of ISO/IEC 29134:2017.

Likelihood can be assessed using the following categories:

- Category I: **Negligible**: Carrying out a threat by exploiting the properties of supporting assets does not appear possible for the selected risk sources (e.g. theft of paper documents stored in a room protected by a badge reader and access code).
- Category II: **Limited**: Carrying out a threat by exploiting the properties of supporting assets appears to be difficult for the selected risk sources (e.g. theft of paper documents stored in a room protected by a badge reader).
- Category III: **Significant**: Carrying out a threat by exploiting the properties of supporting assets appears to be possible for the selected risk sources (e.g. theft of paper documents stored in offices that cannot be accessed without first checking in at reception).
- Category IV: **Maximum**: Carrying out a threat by exploiting the properties of supporting assets appears to be extremely easy for the selected risk sources (e.g. theft of paper documents stored in a lobby).

Impacts can be assessed using the following categories:

- Category I: **Negligible**: data subjects either will not be affected or may encounter a few inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations, etc.).
- Category II: **Limited**: data subjects may encounter significant inconveniences, which they will be able to overcome despite a few difficulties (extra costs, denial of access to business services, fear, lack of understanding, stress, minor physical ailments, etc.).
- Category III: **Significant**: data subjects may encounter significant consequences, which they should be able to overcome albeit with serious difficulties (misappropriation of funds, blacklisting by banks, property damage, loss of employment, subpoena, worsening of state of health, etc.).
- Category IV: **Maximum**: data subjects may encounter significant, or even irreversible, consequences, which they may not overcome (financial distress such as unserviceable debt or inability to work, long-term psychological or physical ailments, death, etc.).

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

Based upon these categorisations, the following data protection risk map can be proposed:

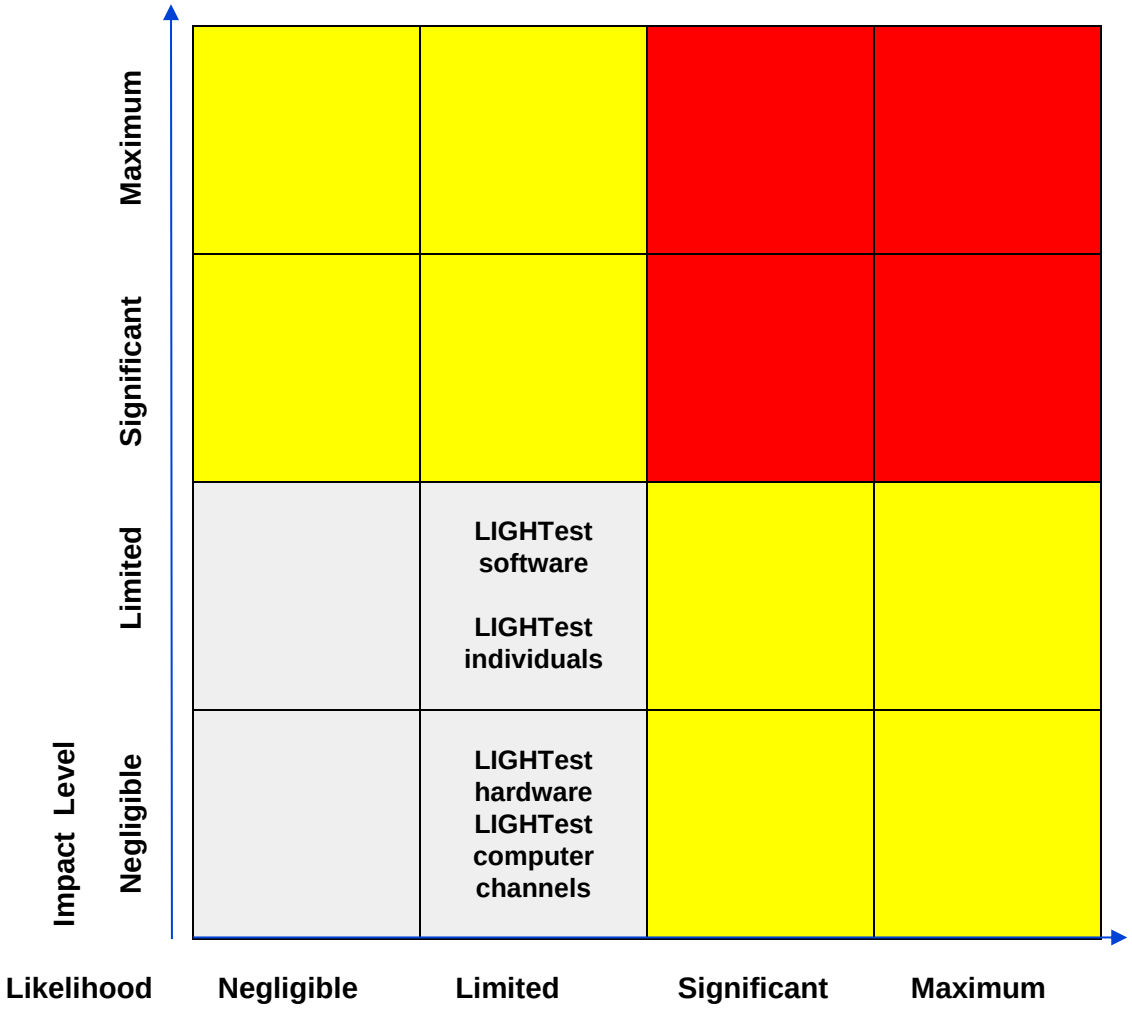

Table 4: Privacy risk map

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

All threats are rated as having a **limited likelihood**, principally due to the consideration that all LIGHTest assets are located under the control of Correos itself, and on the basis that this is a pilot project with relatively small-scale use, and that the data processing itself cannot expose the most sensitive data (actual messages exchanged via Correos). This makes the LIGHTest components an unlikely and unattractive target for attacks.

LIGHTest hardware and computer channel threats are rated as having a **negligible impact,** since the main consequence is that the services of Correos become temporarily unavailable, which is not entirely unacceptable for a pilot project, and more important because fallback solutions exist (in the form of the traditional commercial service provided by Correos). The LIGHTest individuals asset could have a **limited impact:** individual could not be directly stolen or abused (since the content of messages does not pass through LIGHTest), but it would be possible to misconfigure LIGHTest components in a way that causes the infrastructure to malfunction, causing messages not to be sent or received. While this would be visible to the end user (who would not get a confirmation message of a positive transaction) and to Correos, this would be more harmful then a temporary unavailability. Finally, the LIGHTest software assets are rated as having a **limited impact** as well, since this is where malware infections or modifications could be applied that might enable disruption of communications. While this would be visible, interruptions of service could occur.

7.3 Compliance analysis - current and contemplated compliance measures – residual risks

The following compliance measures have been taken to mitigate the risk measures:

- **Purpose restriction:** in accordance with the GDPR, processed data may only be used for the contractual tasks of Correos.
- **Legitimacy and lawfulness:** in accordance with the GDPR, only Correos will be able to process data.
- **Data minimisation principle**: in accordance with the GDPR, personal data will in principle not be processed via LIGHTest infrastructure; only trust policy information. This limits the risk to the data subjects.
- **Transparency and accuracy:** in accordance with the GDPR, all information required is made available by Correos through standardised data protection notices. No further notices are required as a result of the use of LIGHTest, since LIGHTest acts as an internal infrastructural tool (no personal data transfer to third parties)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

- **Integrity and confidentiality**: standard LIGHTest configurations are used, but these are supported by the existing and tested Correos infrastructure, both for ensuring the integrity and authenticity of exchanged messages and to identify end users reliably.
- **Auditing and accountability** are supported through logging practices that allow individual communications and relevant metadata (but not the exchanged messages) to be retained for the duration of the LIGHTest project, that allow exchanges through LIGHTest components to be verified by Correos in case of disputes (including the identification of the sending and receiving parties, the time of the exchange, and the integrity/authenticity of the exchanged data itself).
- **Data location and data transfers:** personal data is stored and processed only within the EU and EEA countries (no personal data sharing in the course of piloting).

Furthermore, while LIGHTest does not inherently improve the processing of personal data by or within Correos before or after using the LIGHTest infrastructure, it is worth noting none the less that LIGHTest enhances data protection in the overall perspective: LIGHTest facilitates automated processing in cases where otherwise trust verification has to be done manually, at least to some extent. Therefore, after the successful implementation of LIGHTest, errors in trust validation can be mitigated. Therefore, personal data risks are generally reduced.

7.4 Conclusions and risk treatment plan

Based on the assessment above, the current practices appear to be substantially compliant with EU data protection law, and are likely to remain so for the duration of the project.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

8. References

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; see http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML; last visited on 12 July 2017

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); see http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32016R0679; last visited on 12 July 2017

Regulation 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 (eIDAS Regulation); see http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG; last visited on 12 July 2017

Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC); see http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32008R0765; last visited on 12 July 2017

APEC Privacy Framework, 2005, https://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx, last visited on 2 August 2017

United Nations Convention on the Use of Electronic Communications in International Contracts, 2005, see http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2005Convention.html, last visited on 2 August 2017

UNCITRAL Model Law on Electronic Commerce, 1996, see http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model.html, last visited on 2 August 2017

UNCITRAL Model Law on Electronic Signatures, 2001, see http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2001Model_signatures.html, last visited on 2 August 2017

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

9. Project Description

LIGHTest project to build a global trust infrastructure that enables electronic transactions in a wide variety of applications

An ever increasing number of transactions are conducted virtually over the Internet. How can you be sure that the person making the transaction is who they say they are? The EU-funded project LIGHTest addresses this issue by creating a global trust infrastructure. It will provide a solution that allows one to distinguish legitimate identities from frauds. This is key in being able to bring an efficiency of electronic transactions to a wide application field ranging from simple verification of electronic signatures, over eProcurement, eJustice, eHealth, and law enforcement, up to the verification of trust in sensors and devices in the Internet of Things.

Traditionally, we often knew our business partners personally, which meant that impersonation and fraud were uncommon. Whether regarding the single European market place or on a Global scale, there is an increasing amount of electronic transactions that are becoming a part of peoples everyday lives, where decisions on establishing who is on the other end of the transaction is important. Clearly, it is necessary to have assistance from authorities to certify trustworthy electronic identities. This has already been done. For example, the EC and Member States have legally binding electronic signatures. But how can we query such authorities in a secure manner? With the current lack of a worldwide standard for publishing and querying trust information, this would be a prohibitively complex leading to verifiers having to deal with a high number of formats and protocols.

The EU-funded LIGHTest project attempts to solve this problem by building a global trust infrastructure where arbitrary authorities can publish their trust information. Setting up a global infrastructure is an ambitious objective; however, given the already existing infrastructure, organization, governance and security standards of the Internet Domain Name System, it is with confidence that this is possible. The EC and Member States can use this to publish lists of qualified trust services, as business registrars and authorities can in health, law enforcement and justice. In the private sector, this can be used to establish trust in inter-banking, international trade, shipping, business reputation and credit rating. Companies, administrations, and citizens can then use LIGHTest open source software to easily query this trust information to verify trust in simple signed documents or multi-faceted complex transactions.

The three-year LIGHTest project starts on September 1st and has an estimated cost of almost 9 Million Euros. It is partially funded by the European Union's Horizon 2020 research and innovation programme under G.A. No. 700321. The LIGHTest consortium consists of 14 partners from 9 European countries and is coordinated by Fraunhofer-Gesellschaft. To reach out beyond Europe, LIGHTest attempts to build up a global community based on international standards and open source software.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460

The partners are ATOS (ES), Time.lex (BE), Technische Universität Graz (AT), EEMA (BE), G+D (DE), Danmarks tekniske Universitet (DK), TUBITAK (TR), Universität Stuttgart (DE), Open Identity Exchange (GB), NLNet Labs (NL), CORREOS (ES), Ubisecure (FI) and University of Piraeus Research Center – UPRC (GR). The Fraunhofer IAO provides the vision and architecture for the project and is responsible for both, its management and the technical coordination.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 737460