LOCARD_D2.5_SELP Continuous Monitoring Report 2_v1.1

Kumar, Ashwinee; Quinn, Paul

Publication date:
2022

Document Version:
Final published version

DELIVERABLE

D2.5 SELP Continuous Monitoring Report 2

Project Acronym:	LOCARD	
Project title:	Lawful evidence collecting and continuity platform development	
Grant Agreement No.	832735	
Website:	https://locard.eu/	
Contact:	info@locard.eu	
Version:	1.1	
Date:	31 October 2022	
Responsible Partner:	VUB, EEMA	
Contributing Partners:	ARC, SAG, APWG, TID, UM, KEMEA	
Reviewers:	Constantinos Patsakis (ARC) Hugo Kerschot (VIC)	
Dissemination Level:	Confidential – only consortium members and European Commission Services	X

This project has received financial support from the European Union Horizon 2020 Programme under grant agreement no. 832735.

1 Revision History

Revision	Date	Author	Organization	Description
0.1	05/01/2022	Ashwinee Kumar, Paul Quinn, Jon Samah	VUB, EEMA	Iteration 4 begins
0.2	16/01/2022	Ashwinee Kumar, Paul Quinn, Jon Samah	VUB, EEMA	Incorporation of Further questions after preliminary analysis of Iteration 4
0.3	16/01/2022	Ashwinee Kumar, Paul Quinn, Jon Samah	VUB, EEMA	Final Responses collected
0.4	17/01/2022	Ashwinee Kumar, Paul Quinn, Jon Samah	VUB, EEMA	Iteration 4 Assessment begins
0.5	14/04/2022	Ashwinee Kumar, Paul Quinn, Jon Samah	VUB, EEMA	Assessment of the responses conducted
0.8	18/04/2022	Ashwinee Kumar, Paul Quinn	VUB	Initial draft
0.9	18/07/2022	Paul Quinn, Ashwinee Kumar	VUB	Internally reviewed and feedback included
0.10	18/07/2022	Constantinos Patsakis, Hugo Kerschot	ARC - VIC	Review remarks
1.0	19/07/2022	Ashwinee Kumar	VUB	Final version
1.1	31/10/2022	Ashwinee Kumar	VUB	Review version

2 Table of Contents

List of Tables

3 Glossary

Terms Specific to LOCARD

Term	Meaning
LEA	Law Enforcement Agency
Local Node	The access point to the LOCARD platform in a particular jurisdiction
Local Node Authority	The authority responsible for the Local Node, especially access policies
Smart Contract	An automated series of code which accompanies each entry onto the LOCARD platform and enforces the policies and conditions determined by the entry originator

Technical Terms

Term	Meaning
API	Application programming interface
Artefact	Object to be tested. In the case of LOCARD: reference architecture; first Implementation; demonstrators and use cases; final release
Blockchain	An immutable storage method utilised by LOCARD
eIDAS	eIDentity Assurance and trust Services regulation (EU 910/2014)
GDPR	General Data Protection Regulations (Directive 95/46/EC)
GUI	Graphic User Interface
IDMS	Identity Management Interface
MoSCoW	Descriptive method to describe Must have / Shall have / Could have /Won't have conditions
SELP	Socio, Ethical, Legal and Privacy

Data Protection Terms

Term	Meaning
Consent of the data subject	It should be a statement or clear affirmative action which is freely given, specific, informed and unambiguous and imitate the wishes of the data subject whereby he/she agrees to the processing of personal data relating to him or her. It can be withdrawn by the data subject anytime; Assessment of free consent can be done via the care of the performance of a contract, provisions of the service agreement.
Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed.
Data Controller	A natural or legal person who, alone or jointly, determines the purposes and means of processing is called data controller
Data Processor	A natural or legal person who processes personal data on behalf on the controller is called data processor

Pseudonymization	Pseudonymization is a kind of processing of personal data in a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information

Detailed descriptions of all terms can be found in LOCARD Deliverable D2.1 SELP Benchmark.

4 Executive Summary

The project LOCARD – Lawful evidence collecting and continuity development platform - is funded by the European Commission through the European H2020 research and innovation programme under grant agreement number 832735.

The work package2, to achieve its objectives under the grant agreement aims to assess the impact of the LOCARD system in terms of social/ethical responsibility, fundamental rights, data protection and privacy. One of its primary objectives is to address any issues identified during the design and the development phase of the project's solutions. Furthermore, it is equally important to strike the proper balance between the legitimate interest and the rights and obligations contained in the personal data protection framework and other legal approaches connected to privacy. This includes the GDPR, case laws of the European Court of Human Rights, and key illustrative examples from the member states of the EU. To this end, legal and ethical requirements should be effectively embedded in the relevant technologies (including on the basis of the data protection by design and default principle (art. 25)). The form of this work package has also been designed to comply with the need to perform an impact assessment as described under article 35 of the GDPR.

This document is prepared under Task T2.4 SELP Continuous Monitoring Report. The aim of this task is to continuously monitor the impact of LOCARD on the requirements identified in the LOCARD impact assessment as the system is integrated, tested, and evaluated. The monitoring has been performed by the VUB. This task has logically followed task T2.3 (Impact Assessment) and the previous version of this deliverable's recommendations. This deliverable ensures that the result of the LOCARD IA and the first monitoring report are implemented by all relevant partners on a continuous basis. The present document forms part of the third main stage of the Social, Ethical, Legal and Privacy (SELP) impact assessment and reports its 4th iteration. This deliverable provides the final report on the monitoring of observance of SELP requirements against the system and on the risk-mitigation strategies implemented thereof by the LOCARD partners. This deliverable covers the activities conducted between May 2021 and July 2022, the period between the submission of deliverable D2.4 SELP Continuous Monitoring Report 1 and its final review. The result of the analysis of the SELP questionnaire-responses also forms part of this deliverable. This report provides a complete picture of evaluation approaches to the SELP requirements, different iterations and their outcome, the necessity of MoSCoW rules in SELP assessments, implementation of recommendations of D2.4 and external advisory board, the status of the previous recommendations, and a summary of the result of the final iteration.

As reported in the "list of deliverables", p – 20 of the GA, the present deliverable is confidential in nature and only available to the members of the consortium and the Commission services. The document was required to be delivered in the M36 of the project, but due to 3 months extension it is submitted in M39 i.e., July 2022.

5 Introduction

Deliverable D2.5 SELP Continuous Monitoring Report 2 is an updated and revised edition of its previous version i.e., D2.4 SELP Continuous Monitoring Report 1 submitted in April 2021. The deliverable forms part of the final phase of the SELP impact assessment (i.e., the first phase was the establishment of the framework, as described in D2.1 SELP Benchmark Report and D2.2 SELP Compliance report, and the second phase was the first iteration of the SELP impact assessment, reported in D2.3 SELP Impact Assessment). The deliverable provides the final report on the monitoring of the LOCARD tools and on the risk-treatment strategies implemented by the concerned LOCARD partners. The document also gives the status of each question subjected to partners for iteration 3 and 4 assessments. It is carried out by VUB and EEMA, in cooperation with the members of the consortium, who contribute to the architecture of the LOCARD platform and its development (i.e., KEMEA, NRS, MOT, ARC, ICO, and IMC).

This document focuses on the Beta release and the final phase of the validation activities, with the specific interest in ensuring observance of SELP recommendations suggested in its previous version. Procedures established in D2.4 to monitor SELP recommendations have been followed to prepare this document. The deliverable takes into consideration the development of the LOCARD system between M25 and M39. This deliverable is the last contribution of WP2. The overall goal is twofold:

- report on the implementation of the recommendations defined in D2.4 and by the External Advisory Board, and
- conduct a SELP impact assessment on the beta release and its components.

To achieve its goal, several deliverables have also been referred for ex. WP4's D4.9 (Research Contribution and Innovation Report) & D4.10 (Source code and data repository), WP5's D5.5 (Release candidate and associated manual) & D5.6 (Final release and associated manual), and WP6's D6.2 (LOCARD Detailed Implementation Plan) and D6.3 (LOCARD Deployment and Validation Report).

6 Evaluation approach to the final version of SELP Continuous Monitoring

The purpose of the final monitoring is to ensure that all previous recommendations related to Societal, Ethical, Legal and Privacy (SELP) requirements are implemented by LOCARD WPs and the consortium, in general.

The LOCARD evaluation approach has examined three differing artefacts: The LOCARD Reference Architecture (responsibility of WP3), Initial implementation (responsibility of WP5), and Demonstrators (responsibility of WP6).

To this end, we used a simple evaluation process in three steps. First, we have identified each of the Artefacts, which in their case are three use cases, a reference architecture, and implementation. Second, we clarified the SELP requirements and expectations for each of the artefacts as developed from deliverable D2.1. Lastly, we evaluated, when each artefact identified was tested against the SELP requirements. The current appropriate artefacts have been re-evaluated and reported in the present deliverable D2.5 SELP Continuous Monitoring Report 2.

Because of the delays in delivering the initial artefact, the initial evaluation (Iteration 1) was repeated (Iteration 2) to ensure that a valid assessment within the intended D2.3 delivery timescale. A summary of iteration 2, for comparison to iteration 3, is included in this deliverable D2.4 as an appendix, together with Iteration 3. Similarly, a summary of iteration 4, for comparison with iteration 3, has been provided in section 7 of this document.

To maintain unambiguity in requirements, the MoSCoW method was introduced for the early evaluations (SELP Impact assessment Monitoring). Being outcome-focused, the method provides a clear and measurable set of specifications, which can, over time, be continually monitored for compliance. The method labels each specific requirement, making it easier to prioritise (as the process proceeds, the evaluation focuses on specific issues that have arisen, resulting in a slightly different set of questions where the MoSCoW methodology appeared less useful).

These impact assessment analyses aimed to identify any SELP failings and weaknesses of the LOCARD platform as it is developed and to stimulate additional consideration of SELP within the overall design. Table 1 represents the initial classification and MoSCoW labelling of iterations 1 and 2 of the SELP requirements. Iteration 3 evolved to a more specific and detailed assessment where MoSCoW was less appropriate.

Condition	Number of Requirements
MUST have	25
SHOULD have	16
COULD have	5

Table 1: MoSCoW Requirements[1]

6.1 Iteration 1:

High Level Results – by number of responses – At Iteration 1

Condition	Number of Requirements	Number of Passes	Number of Neutral	Number of Fail	Number Not Applicable
MUST have	25	9	10	0	6
SHOULD have	16	6	6	0	4
COULD have	5	3	2	0	0

Table 2: Distribution of SELP Impact Assessment Analysis against MoSCoW requirements at Iteration 1

High Level Results – by percentage – At Iteration 1

Condition	Number of Requirements	Number of Passes	Number of Neutral	Number of Fail	Number Not Applicable
MUST have	25	36%	40%	0%	24%
SHOULD have	16	37.5%	37.5%	0%	25%
COULD have	5	60%	40%	0%	%

Table 3: Distribution of SELP Impact Assessment Analysis against MoSCoW requirements at Iteration 1

6.2 Iteration 2:

High Level Results – by number of responses – At Iteration 2

Condition	Number of Requirements	Number of Passes	Number of Neutral	Number of Fail	Number Not Applicable	Number Not Known
MUST have	25	4	13	0	2	6
SHOULD have	16	6	7	0	0	3
COULD have	5	1	3	0	0	1

Table 4: Distribution of SELP Impact Assessment Analysis against MoSCoW requirements at Iteration 2

High Level Results – by percentage – At Iteration 2

Condition	Number of Requirements	Number of Passes	Number of Neutral	Number of Fail	Number Not Applicable	Number Not Known
MUST have	25	16%	52%	0%	8%	24%
SHOULD have	16	37%	44%	0%	0%	19%
COULD have	5	20%	60%	0%	0%	20%

Table 5: Distribution of SELP Impact Assessment Analysis against MoSCoW requirements at Iteration 2

[1] To know more about LOCARD MoSCOW requirement, please refer LOCARD deliverable D2.3 SELP Impact Assessment

6.3 Numeric identification of each requirement for iteration 3 & 4

With a large number of assessments and requirements presented during the course of the project, a numbering system was required to ensure the correct identification of the issue. For this purpose, the following identification has been used.

- Topic
- Iteration number
- Revision (Revision '2' designates a supplementary question)
- Requirement number

For example: *SELP: 4.1.01 or SELP:4.2.01*

Ref. Number (At Iteration 3)	Status at Iteration 3	Ref. Number (At Iteration 4)	Status at Iteration 4
SELP:3.1.001	Compliant	-N/A-	-N/A-
SELP:3.1.002	Neutral	SELP:4.1.002	Compliant
SELP:3.1.003	Neutral	SELP:4.1.003	Compliant
SELP:3.2.003	Neutral	SELP:4.2.003	Compliant
SELP:3.1.004	Neutral	SELP:4.1.004	Compliant
SELP:3.1.005	Fail	SELP:4.1.005	Compliant
SELP:3.1.006	Neutral	SELP:4.1.006	Compliant
SELP:3.1.007	Neutral	SELP:4.1.007	Compliant
SELP:3.2.007	Compliant	-N/A-	-N/A-
SELP:3.1.008	Neutral	SELP:4.1.008	Compliant
SELP:3.1.009	Neutral	SELP:4.1.009	Compliant
SELP:3.1.010	Neutral	SELP:4.1.010	Compliant
SELP:3.1.011	Neutral	SELP:4.1.011	Compliant
SELP:3.1.012	Compliant	-N/A-	-N/A-
SELP:3.1.013	Neutral	SELP:4.1.013	Compliant
SELP:3.2.013	Compliant	-N/A-	-N/A-
SELP:3.1.014	Neutral	SELP:4.1.014	Compliant
SELP:3.1.015	Neutral	SELP:4.1.015	Compliant
SELP:3.2.015	Neutral	SELP:4.2.015	Compliant
SELP:3.1.016	Neutral	SELP:4.1.016	Compliant
SELP:3.1.017	Compliant	-N/A-	-N/A-
SELP:3.1.018	Neutral	SELP:4.1.018	Compliant
SELP:3.1.019	Compliant	-N/A-	-N/A-
SELP:3.1.020	Compliant	-N/A-	-N/A-
SELP:3.2.020	Compliant	-N/A-	-N/A-
SELP:3.1.021	Neutral	SELP:4.1.021	Compliant
SELP:3.2.021	Neutral	SELP:4.2.021	Compliant
SELP:3.1.022	Neutral	SELP:4.1.022	Compliant

SELP:3.1.023	Compliant	-N/A-	-N/A-
SELP:3.2.023	Compliant	-N/A-	-N/A-
SELP:3.1.024	Compliant	-N/A-	-N/A-
SELP:3.1.025	Compliant	-N/A-	-N/A-
SELP:3.1.026	Compliant	-N/A-	-N/A-
SELP:3.1.027	Compliant	-N/A-	-N/A-
SELP:3.2.027	Compliant	-N/A-	-N/A-
SELP:3.1.028	Compliant	-N/A-	-N/A-
SELP:3.1.029	Compliant	-N/A-	-N/A-
SELP:3.1.030	Compliant	-N/A-	-N/A-
		SELP:4.1.032	Compliant
		SELP:3.1.033	Compliant
		SELP:3.1.034	Compliant
		SELP:3.1.035	Compliant
		SELP:3.1.036	Compliant
		SELP:3.1.037	Compliant
		SELP:3.1.039	Compliant
		SELP:3.1.040	Compliant

Table 6: Status of each referencer on SELP requirements at Iteration 3 & 4

7 Iteration 4

7.1 Methodology

The basic methodology established for assessing the impact of the LOCARD system and followed up in the previous version of this document i.e., D2.4 SELP Continuous Monitoring Report 1 has been reiterated here. However, a few modifications have been made:

- The questionnaire-response that was analysed previously as fail or neutral has been taken into consideration for further monitoring.
- As the number of follow-ups/monitoring questions/open issues were reduced, the number of respondents has been equally shortened.
- The questions themselves have been refined to meet any specific issue that needs to be addressed.
- A total of 28 questions (based on the open issues/to be followed-up) were chosen to be addressed to the LOCARD consortium. Out of these 28 questions, 8 are newly added at the Iteration 4 stage that focuses on the rights of data protection and the LOCARD technology, especially Blockchain.
- The final monitoring is focused on the LOCARD system rather than each work package (WPs).
- The analysis of responses for the final monitoring of an SELP issue considers both the advancement made against that issue until iteration 4 and the response provided at iteration 3. This rule also applies to follow-up questions.
- The result (Pass/Fail/Neutral) against an open SELP issue at iteration 4 is the outcome of the analysis of all responses available for that issue so far, except the newly added questions.
- Apart from the usual practice of issuing questionnaires for the final monitoring, separate email communications have also been established with the concerned partners where additional information was required.
- For the sake of convenience, results are grouped against the open issues and under specific topics/modules.

7.2 Monitoring of Artefact 2

Iteration 4 is the second iteration to examine the development of Artefact 2 and to monitor the observance of SELP recommendations. The core LOCARD modules that have been tested against the SELP requirements and issues related to any of those modules assessed previously as ‘neutral’ or ‘fail’ have been reassessed at this stage. These modules are:

- Intelligent Crawler
- Investigators’ Toolkit
- Communication Engine
- Crowdsource Intelligence
- Storage Manager
- Blockchain Manager
- User & Identity Manager
- Deviant Patters Repository

Those LOCARD modules, and issues related to them, that have successfully passed the SELP requirements test either at the Iteration 3 analysis or before the beginning of Iteration 4 have been excluded from the final monitoring.

8 Implementation of the recommendations of D2.4 SELP Continuous Monitoring Report 1

As far as work package-specific recommendations are concerned, either they have already been met with and summarized in the previous version of this deliverable or are kept open to be monitored until the preparation of this deliverable. As the previous recommendations, those who are open, could not be implemented separately; they have been thoroughly dealt with and are part of the deliverables of the concerned partner. Below is the implementation status of the previous recommendations, WPs-wise.

8.1 Work Package 2

It was recommended in the last monitoring report (D2.4 SELP Continuous Monitoring Report 1) that Future Users of LOCARD should be provided with the SELP guidelines. The guidelines are already prepared and implemented under the document titled "LOCARD Social, Ethical, Legal and Privacy (SELP) Assessment Handbook for End-users". The handbook covers all necessary guidelines that will help the LOCARD end-users to protect data subjects' rights related to privacy and data protection and in the ethical use of the LOCARD platform. Also, on top of the SELP handbook, WP5 has produced two deliverables as guides on how to operate the LOCARD platform. The deliverables are D5.5 Release candidate and Associated Manual and D5.6 Final Release and Associated Manual, submitted in October 2021 and July 2022, respectively.

8.2 Work Package 3

When preparing the 1st monitoring report, WP3 was told to provide reports on LOCARD deletion mechanisms, LOCARD privacy by design techniques, and LOCARD data protection by design and default techniques. Based on these SELP requirements, WP3 came forward with a set of documents that speaks about LOCARD's physical architecture and data centres. The monitoring report found the steps taken as appropriate and aligned with the SELP requirements established in deliverable D2.1. There was no specific recommendation under D2.4 to be followed up for WP3, except to participate in the Iteration 4 questionnaire to show whether the tasks assigned to this WP have been completed. The iteration 4 questionnaire-response and analysis are part of Section 7 of this document.

8.3 Work Package 4

It was observed in the first monitoring report that the stakeholders (users) of LOCARD could be the best option to validate the necessity and significance of the platform. Therefore, an action plan was proposed to be taken to fulfil certain objectives:

- That the outcomes of the action plan should provide a pathway to assess the LOCARD platform from stakeholders' perspectives leading to the current technology landscape.
- That the actions of the plan should provide a justified method to identify the metrics of subjective evaluation of LOCARD which is easy to validate the stakeholders' requirements.
- That it identifies the areas where LOCARD can improve its productivity over existing digital forensics practices.
- That it helps in revealing the inefficiencies and unnecessary technology adoption in any part or module of the present LOCARD platform.

- That it identifies after the assessment about the stakeholders' coherent plan for technological enhancements for LOCARD, in other words digital forensic readiness for LOCARD.

As the actions proposed to meet these objectives were interrelated, WP4 and WP6 have implemented all action plans necessary to validate and discuss the significance of the LOCARD platform. To achieve the goals, WP4 deliverables D4.9 (Research Contribution and Innovation Report) – an updated version of D4.7 - & D4.10 (Source code and Data Repository) cover all action plans proposed in D2.4, of course, related to this work package. Furthermore, work package WP6 in its deliverables D6.2 (LOCARD Detailed Implementation Plan) & D 6.3 (LOCARD Deployment and Validation Report) provide a detailed landscape of LOCARD testers, users and stockholders, their roles and responsibilities, Use Cases and legal formalities, LOCARD testing and validation methodology procedures, and testing & validation outcomes.

8.4 Liability Impact Assessment

D2.4 SELP Continuous Monitoring Report 1 held that the role of the system administrator would be essential as it will be able to determine multiple parameters of use. Such roles and responsibilities will be incorporated and discussed in the manual of the platform, to be reported in D5.6 Final release and associated manual. The consortium, through WP5, has produced both deliverables D5.5 Release candidate and Associated Manual and D5.6 Final Release and Associated Manual. The former deliverable provides a very detailed and comprehensive LOCARD Installation Guide, including Keycloack, and User Manual for core LOCARD tools such as Crowdsource Intelligence, Storage Manager, Blockchain Manager, User & Identity Manager, TUB Network forensics tool, TUB Side Channel Extraction tool, NTNU IDNA tool, TUB Tool Hardware-OS, UNIPD SMS-based forge ID tool, UNIPD Vulnerable app identification tool, UNIPD Spyware apps identification tool, UM Device hijack investigation tool, Intelligent Crawler, Smart Contract, etc. The Liability Impact Assessment, for the future user of the LOCARD platform, carried out on the content of the LOCARD Installation Guide and User Manual, appreciates the steps taken by the consortium. The LOCARD future users will be benefited further by referring the installation guide and user manual with the LOCARD implementation plan.

8.5 Evaluation of Response

The recommendations proposed in D2.4 SELP Continuous Monitoring Report 1 have been duly taken into consideration by the required Work Package leaders and have been integrated/implemented in the LOCARD platform, as well as in the project. No previous recommendation is open at this stage of the project. Until the submission of the present report (M39), the work of the consortium concerning the follow-up of D2.4 is fully satisfactory and aligned with the SELP requirements set out in WP2's deliverable D2.1 SELP Benchmark.

9 Implementation of the recommendations of the External Advisory Board

The External Advisory Board of the LOCARD project was consulted to review the SELP deliverables and to provide recommendations in order to ensure adherence to the LOCARD SELP requirements. The Board, in its July 2021 report, recommended certain actions to be followed up by the consortium to fulfil high-level legal and ethical standards at a global scope. The recommendations were:

R1: Elaborate a report about potential misuse of the LOCARD tools and share with the EAB for further comments and suggestions.

R2: Although this falls outside the boundaries of the LOCARD project itself, we recommend that the consortium elaborate a 'policy' document, such as a shared understanding or commitment on the terms for further use of the LOCARD-produced tools beyond the end of the project, to ensure that a clear understanding is outlined & shared on the high ethical and privacy standards that the consortium considers necessary for a fair and effective deployment of the tool.

R3: One hot topic, not only related to the project itself but to the technology used, is the one related to the use of Blockchain. The fact that evidence is stored and cannot be deleted may pose a problem to comply with data protection regulations. We recommend the partners to discuss such an issue.

In response to these recommendations, the LOCARD consortium was invited to address these issues. Several public deliverables from WP1, 2, 5, and 8 were presented before the Board for further assessment and observation. The Board, in its updated report of June 2022, made the following observations against the respective recommendations:

O1: The consortium has considered our suggestions and adopted different ways to handle misuse of the LOCARD tools and Platform. Section 3.2.3 of deliverable D1.7 "Responses to Second Ethics Check Report" discusses the potential misuse of the LOCARD tools from different perspectives. First, the following questions are addressed: "Could the component or the system harm individuals (in terms of SELP requirements) if they are modified or enhanced?"; "What would happen if the component or the system would end up in the hands of malevolent individuals?"; "Could the component or the system serve other purposes than the intended applications?"; "Is it possible to misuse the component or the system due to the lack of knowledge?". Moreover, the deliverable details the possible forms of misuse (intentional and unintentional), and their respective preventive measures (proactive and reactive). The said section of the deliverable contains an in-depth discussion about misuse of tools from the LOCARD architecture and the system design points of view. The deliverable D1.7 has been shared with the EAB, and we are satisfied with the steps taken by the consortium.

O2: The consortium has developed a very concise and easy to understand document/slides entitled "LOCARD Social, Ethical, Legal and Privacy (SELP) Assessment Handbook for End-users" that provides a good understanding of the LOCARD tools and system in terms of ethical and privacy standards.

O3: The LOCARD project has taken into consideration the issues related to deletion of a piece of information while using Blockchain. The LOCARD system provides the end-users the flexibility required to apply the data deletion mechanisms validly and to respect data subject's rights according to the GDPR. Essentially, evidence is not stored in the blockchain: it only stores the necessary data to allow the retrieval of evidence from the corresponding storage media. Regarding the measures for collecting and managing

sensitive and personal data considered in GDPR, these have been addressed in LOCARD. Note that since the platform stores information that, in principle, is a part of an investigation, this information cannot be erased just because someone requested to exercise his right to erasure. Since LOCARD does not store the data per se in the blockchain, but in storage media "outside the blockchain" the destruction of the data can be made from the corresponding entities as it would normally happen, that is when the corresponding legal framework considers that the case moves to the disposal phase. At that point, the status of the case is changed in the LOCARD blockchain accordingly, access to hashes is automatically dismissed with the smart contracts and the corresponding entity destroys the data following the disposal protocol.

10 Results – Iteration 4

This section provides a summary of the communications, both through the questionnaire and emails, established with the LOCARD partners to monitor the development of the system by implementing SELP requirements. The summary of communications includes questions, supplementary questions, responses and the status of each response; pass (compliant), fail (non-compliant), and neutral. The communication for the monitoring purposes spans from M32 to M38. The LOCARD consortium has been successful in implementing all recommendations against SELP requirements. At this final stage of monitoring, no issue comes under the 'fail' or 'neutral' categories. Here, only those questions and their respective responses are presented that were open to being monitored throughout the lifecycle of the project because of their falling in the 'neutral or fail' category. As the Blockchain's debatable characteristics and previous recommendations from the EAB, several new questions on it were subjected to the consortium that was not part of the previous iterations. The analysis of the responses of the LOCARD consortium on these questions found that the LOCARD blockchain tool poses no threat to the data subject's rights. As followed in the previous version of

this document, primary questions, follow-up questions, and their responses are presented just below the core LOCARD module/component. Colour coding has been used to indicate the evaluation status of the questionnaire-response at iteration 4: green (pass), blue (neutral), and fail (red). A result/status marked in green means compliance with the SELP requirement. The rest two colours indicate non-compliance with those requirements. As the consortium implemented all recommendations in developing the SELP-compliant LOCARD system, the current evaluation status falls in the green colour code category. This suggests that the LOCARD system and its tools fulfil all SELP requirements set out in deliverable D2.1 SELP Benchmark Report. The system is able to respect the data subject's privacy and data protection rights and existing EU legal regimes and ethical standards. For the purpose of general understanding, the development status of a particular LOCARD module at iterations 3 & 4 is also provided.

Ref. number	Question	System module/Answer	Recommendation/Follow up question [After Iteration 3]	Follow up response [On Iteration 4]	Status - Recommendation [At Iteration 4]
Intelligent Crawler (ICO) [At Iteration 3] The LOCARD crawler provides an interface to facilitate evidence collection from the Internet, using HTTrack. HTTrack allows you to download a World Wide Web site from the Internet to a local directory, recursively crawling all directories, storing HTML, images, and other files from the server to your computer. HTTrack stores its results by default in the local storage but this can be controlled with the help of the -O flag in the HTTrack executable. In this way any location can be used as a storage back-end including network drive or services like SFTP. Crowdsource intelligence inputs can be used by the Intelligent Crawler to search for malicious content in specific sites. Such collected evidence will then be stored and processed by the Investigator's Toolkit and/or the Deviant Pattern Repository accordingly. Note that the corresponding interactions will be logged into the blockchain, while alerts will be raised when new evidence is collected. [At Iteration 4] The Intelligent Crawler is an important module for searching the web. httrack website copier (www.httrack.com) is used which has many useful features like indexing a site according to the number of occurrences of a specific keyword indicating at the same time the page and the number of occurrences the keyword has been found within the page.						
SELP.V4.1.002	When will the mirrored website be deleted? Is it automatic or manual deletion? Who is responsible for the deletion	No, there is no automatic deletion mechanism. The person who has access to the location will be in charge to manually delete the mirrored site.	The responsibilities of the authorized person should be clear. Data erasure should happen as soon as possible. Automatic deletion mechanisms should be revised and considered.	The deletion of an evidence is managed by the investigator(s) if applicable. It will follow the same procedure than evidence, once in a case it can only be deleted or erased in some specific occasions, mostly at the end of a case. A mirrored website, from the moment it	**Compliant** - It is advised to adopt a plan that clearly figures out the responsibilities of the investigator(s) regarding management of mirrored

	mechanism?			is collected in the context of a case and thus becomes evidence, is no exception.	website, including data deletion. The plan should include policies equally applicable to all investigators, throughout the LOCARD system. There should not be any fix policy that the mirrored website can only be deleted at the end of some specific cases. Once the purpose of the data collection is met, the website should be deleted without undue delay. Automatic deletion mechanisms should be adopted and worked upon to make the LOCARD

					system robust.
SELP.V4.1.003	The mirrored website or parts thereof will be copied to the Investigator's Toolkit and/or the Deviant Pattern Repository and the HTTrack will delete the mirror. Does this deletion depend only on the fact of the copy?	One can directly copy the site to the aforementioned tools (indicate a location accessible by the tools). What is implied with an investigator's toolkit? For the tech team the investigator's toolkit is the set of tools by research organizations. No such integration has been foreseen so far with the deviant pattern repository.	The responsible person should be assigned with the related tasks and obligations to ensure the deletion and post-analysis processes are executed.	The data mirrored will be stored as evidence and it will be analysed either via the LOCARD platform or locally by the investigator. The platform works in a simpler fashion. The website is mirrored and stored as evidence. If a URL is queried from the deviant behavior the functionality is the same.	**Compliant -** Whoever will be responsible for the analysis and whatever will be the mode of that analysis, deletion must be ensured. A guideline should be made available to the investigator(s) about which mode of analysis, either through the LOCARD platform or locally, will provide greater legal compliance.
SELP.V4.2.003	Does the HTTrack mirrored site have any use once the content is copied to the investigator's toolkit?	Yes, data is kept there until it is no longer necessary.	As there is no automated deletion mechanism in the platform and data is proposed to be kept as long as it is necessary (i.e., until the end of a criminal case) internal policies should include the technical details of deletion. Altogether, it is preferable to include a way in the platform to dispose of the evidence (as a	If there exists a copy in the evidence dataset, any temporary files can be dismissed. Thus, it can be later used and analysed accordingly.	**Compliant –** A data retention policy should be defined.

			function). The authorized user should be able to delete once the case is closed and data is no longer needed.		

Investigator's Toolkit (MOT)

[At Iteration 3] This is a set of offline forensic tools whose output is automatically bridged with the Storage manager. The tools allow investigators to perform their usual data acquisition and analysis procedures. However, in this case the tools' output is stored along with the evidence. Moreover, the credentials of the user are also linked to such forensic output to enable auditing as well as committing each investigator to his findings. These outputs will be files or sets of files and summary reports when eligible. The latter will be processed by the Reporting Engine in order to create the final documentation of a case. The Investigator's Toolkit interacts with the following modules:

- Alert Engine
- Storage Manager
- Intelligent Crawler
- Deviant Patterns Repository
- LOCARD Reporting Engine
- LOCARD Blockchain
- LOCARD UI/UX Interface and Portal
- LOCARD TEE

[At Iteration 4] The investigator toolkit incorporates a set of forensic tools which have been developed by LOCARD University partners. There are three (3) broad categories of such tools, namely:

1. tools for streaming forensics
2. tools for cloud forensics
3. tools for mobile forensics

SELP.V4.1.004	Will the forensic tools be used during the project on real data?	So far, we know it will be synthetic data. This though will be further elaborated and agreed during wp6 testing protocols to be agreed.	This should be put on hold as there is no definite answer now. Could be changed by the outcome of WP6? WP2 & WP6 should be informed. On hold until further clarification in WP6. It should be verified later stages of the project as well.	According to the discussions among partners in WP6, dummy data will be used throughout the first validation and piloting activities. No real data will be used. This is stated in the Data Management Plan of the project as well.	**Compliant** - Any change in this plan should be discussed first and assessed according to the SELP benchmarks .

Communication Engine (MOT) [At Iteration 3] The LOCARD portal will incorporate the possibility to send an email to a specific user. The main use of this communication is to request further details of a specific evidence, report, or case from other LOCARD users. The Identities of the users will be managed by the ID management module, and the requirement that these are anonymized will be discussed with the end users and assessed during the project. The communication Engine interacts with the following modules: • LOCARD UI/UX Interface and Portal • LOCARD Blockchain [At Iteration 4] As required by many end users, the possibility of communication between LOCARD users is a desirable feature. To this end, LOCARD aims to allow investigators to publish some evidence, so that others can find similarities. In this case, the Communication Engine will allow them to exchange information, should they be given this permission, and log all the corresponding messages.					
SELP.V4.1.005	Where will the mails be physically stored (both during the project and in real life setting)? How will they be tamper-proof?	Mails between users in the same node are saved in MariaDB database. Mails between users in different nodes is still pending if they will be implemented and where will they be saved. As for tamper-proof mails so far mails within a node are security protected based on inherent BPM software security controls.	The storage and security measures of mails between users at different nodes should be clarified. Suggestion: Registered email by EIDAS if possible and implementation of a function enabling to receive, record and store external emails on LOCARD as per security of the VPN.	The mails if they are collected as evidence during an investigation have the same applicability than any evidence. About the communication between investigators, since the chat is for general purpose, nothing is logged as an evidence in any case. Note that the information could refer to distinct cases in the chat. The internal communication has a similar purpose that other messaging system such as Skype, but it is executed inside of the platform for security and privacy reasons. However, the investigators, if desired, could manually create a transcript of any specific part and upload it as a new	**Compliant** - Similar protection should be provided to the emails as well that contain general-purpose chats. In a case where email chat can be used a court, it becomes necessary to protect it from tampering since its inception. A mechanism must be adopted to protect emails from tampering.

				document in this case.	
SELP.V4.1.006	Can these emails be extracted to be used at the court?	So far we know that any information going to a third party is retrieved from the smart contract. So far no mails are stored in the smart contact.	Any mails must be added to the smart contract.	Depending on their scope, if these are introduced as evidence in the system, the procedure to do so will follow whatever procedure the current investigators follow (e.g. creating a certified copy, requesting further details to the email provider, etc).	**Compliant** - It is advised that email chats should be added to the smart contract.
Crowdsource Intelligence (MOT) [At Iteration 3] This module is mainly focused on collecting intelligence from the general public / citizens. To this end, citizens - after registering - will be able to report content such as abuse over a social network (public feeds) or illegal streaming content (child pornography, IP infringement etc.). To allow general public / citizen reporting, a web form will be designed and accessed through the main LOCARD portal which will incorporate user authentication mechanisms to prevent service abuse, spam and DoS attacks. Once the proper information is received, the information will be forwarded to the LEA Area Coordinator that will manage the information and distribute it accordingly or assign it to other end users. The type of information initially collected by the module will need to be sufficient to be assessed and will need to be consistent with GDPR and other local jurisdictional requirements. The exact details are outside of the scope of the LOCARD project, but in practice will need to be acceptable by all participating jurisdictions, and so may need to be centrally managed. [At Iteration 4] This module is about collecting digital crime incidents data reported from the general public/citizens and organisations, hence of great importance. To this end, citizens and organisations will be able to freely report content related to digital crime incidents.					
SELP.V4.1.007	What information is requested from the users during registration? Where is the user data stored	No registration is needed as it was agreed between partners. Data is stored on the MariaDB database of the LOCARD system.	Registration processes (or the lack thereof) should be described in the user manual.	This is detailed in the Deliverables where the Crowdsource engine is described. Data are stored during the scope of an investigation if needed, applying the same policies than current organisations would apply. The	**Compliant** - The approach adopted by the LOCARD system policy in this regard is appreciated.

	and until when?			decision is not forced or limited by LOCARD, and relies on the owners of such data, which will be the recipients of the petition, namely each organisation(s). When deployed, each organisation will manage these details. LOCARD does not force or impose a policy.	
SELP.V4.1.008	Do you have policies and info sheets in place for the users? Who can access the users' profile?	Yes, we have policies but not info sheets yet as these info sheets are part of the user manual which will come later in the project with the first version end of April 2021. User profiles will be accessed ONLY by the admin person responsible from each end user.	Information sheets should be drafted as part of the user manual (D5.5 and D5.6). This should be the same for every node.	Dependent on users. Citizens – The crowdsource engine offers the same capabilities than typical LEAs or similar when collecting information. User's profiles and data facilitated during the process will be accessed by whoever is in charge of such a petition and thereafter a possible investigation. Users have their right to be deleted from the system applying GDPR policies, yet if they are part of an investigation and some data is relevant to it, it will remain according to the investigation needs. This will be assessed by the corresponding organisation. The	**Compliant**

				LOCARD blockchain itself stores only referenced hashes.	
SELP.V4.1.009	Do users have criminal liability when using the system (e.g., false accusation)?	Not aware of this	This reflects a similar T&C's to the non-automated chain of custody in the currently in use. This should be addressed by future users of the LOCARD platform. Also, it should be mentioned in the user manual.	This is out of the scope of LOCARD. The corresponding laws will apply according to each jurisdiction.	**Compliant -** The LOCARD system user manual must incorporate policies regarding criminal liability for the users in the case when a false accusation is made by the user itself or when the user allows such accusations to the system knowingly. A clarification on this account should be provided in the user manual.
SELP.V4.1.010	If the exact details are outside the scope of the project (as stated in D3.5 p21),	Not defined yet.	D3.5 p21 to be followed. There should be a pop-up or a link stating 'Do you accept the following T&C's…'.	It is out of the scope of LOCARD.	**Compliant**

	where are the actual boundaries thereof?				
SELP.V4.1.011	Is there any actual testing foreseen during the project? How do you ensure the adequacy and user-friendliness of the platform?	Yes, there will be several testing cycles taking place. First tests start beginning of February on a dedicated node for this reason. These tests will run from wp6 team in cooperation with the technical team. Further tests will start as from May 2021 with the end users using the system from their own dedicated LOCARD nodes.	WP6 should provide more information about the tests foreseen in connection with the crowdsource intelligence module (to be included in D6.1 Testing and validation protocol).	There are several testing activities, as part of WP6. The UI/UX have been designed according to several well-known development mechanisms. These details are stated in the different deliverables of WP5, and specifically in the Architecture deliverable D3.5.	**Compliant** - Requirements are met.
Storage manager (NRS) [At Iteration 3] This module consists of several databases which store different types of data. Apart from the evidence storage (which will be different according to each end user requirements) as well as its proper access mechanism (API or SFTP service), this module will be used for giving users the ability to store metadata of cases/evidence. Users will select either to store this data on their own premises offline or in this distributed storage, consisting of nodes hosted in all end user's premises. Every organisation will host a node in their own premises and all these nodes will be interconnected. Data will be stored across regions and jurisdictions and all nodes will be participating in the consensus algorithm. Users can interact with storage instances through APIs provided by each instance. [At Iteration 4] The storage manager provides a distributed database which features high availability, consistency and scalability, acting as a supplementary role of a unifying distributed storage layer.					
SELP.V4.1.014	Will the storage be tested with real data during the project?	It can be tested. Whether this will be done is a consortium decision and so far, we have agreed on using synthetic data.	On hold, to be verified.	No personal data nor data coming from any real investigation will be used.	**Compliant**

SELP.V4.1.015	At what stage of the criminal procedure (and the use of LOCARD) is the data transferred to this repository? Until when is it kept there?	Every time we have new evidence, this data is sent to the smart contract and the storage manager.		As each step is logged into the blockchain contemporarily, any modification or deletion of an evidence, regardless of their relevance, will be audited.	**Compliant** - The audit mechanism adopted to keep the system legally compliant is highly appreciated. However, a pre-audit and pre-modification/deletion stages policy should also be adapted to provide real-time protection to the rights of the data subject, for ex. 'right to rectification', 'right to erasure', etc.
SELP.V4.2.015	Please provide a further clarification in regard to relationships to off-chain storage and blockchain information pointers?	Create an interaction with the blockchain, containing some metadata (hash). Can be correlated with a piece of evidence.	Consider the recommendations to SELP.V3.1.003 concerning the deletion mechanisms and responsibilities.	The blockchain stores hashes in a tamper-proof manner, which are later used by other components of the platform. This way auditability and verifiability are ensured. Other data stored in the transactions, such as investigator ID and use case ID can be used to further locate and ease reporting and audits.	**Compliant**

Blockchain Manager (NRS)

[At Iteration 3] This module is in charge of managing the LOCARD blockchain network and issuing the smart contracts that will enable end user's interaction and describe the specific actions that a user can issue on the blockchain. The goal of the Blockchain Manager is to initialise a federated permissioned blockchain system, manage the users and their transactions and cater to the automatic generation of the Smart Contracts. In this regard, LOCARD will allow the participating entities to use a predefined set of Smart Contract as skeletons that will meet the end-user requirements.

[At Iteration 4] The goal of the blockchain manager is threefold, namely:

1. successfully create the blockchain network. The network will compromise nodes for each of the end users participating in the project.
2. to deploy the smart contract to the network which will provide much of the functionality for the LOCARD project.
3. to provide an API which will interact with the smart contract, and which authorises a user. Then this user will be able to interact with the blockchain network.

SELP.V4.1.016	Who will overview the applicability and compliance of smart contracts during and after the project?	A blockchain network is being consisted of multiple nodes that each one of them resides in each jurisdiction separately. Smart Contract (which is the actual data contract between all participants) cannot be enforced from one to another participant. Each participant will receive the smart contract in order to review it and upload it himself to his node. The same version of a Smart Contract must be installed from both six participants in order the network to be	The supervising authority should be identified and allocated as one of their own.	It will depend on each jurisdiction and what organisations will be part of the whole ecosystem. This would entail assessing them in any post-LOCARD governance discussions.	**Compliant** - The LOCARD governance model should devise a plan wherein the responsibilities are clearly demarcated against the authority, for ex. DPA in a jurisdiction.

		valid. This is calculated by a hash algorithm that ensures this uniqueness. So, since no one in the network can enforce by himself the change of a smart contract (for example next version), each time there is a need for change in favour of compliance or applicability then all 6 participants they will receive the revised version of a smart contract which they will review again and install it themselves in their own node (because only them have access to it).			

User and identity Manager (NRS)

[At Iteration 3] User Management in LOCARD is going to be implemented by a custom OAUTH2 Service which will define access, rights, roles and segregation of data for every user. This will be achieved by an OAUTH2 Server based on Java and Spring Security. OAUTH2 Server will rely on a Maria DB database which will hold credentials information for every user. When a user login successfully through this service he will receive an access token. This token, a JSON Web Token (JWT), will be valid for a short period of time and will define the role of a user inside the application. MariaDB will also keep the public keys for each organization's users in Blockchain. Identity Manager will handle access to the app giving the users the ability to have a normal login procedure (username, password). At the same time when a user requests info from Blockchain or does an action to it, in order to accomplish that, the identity manager will retrieve his private key from the database and provide it to the Blockchain API to make any transactions. Like this we create a middle application layer that connects users to their keys in Blockchain. Also, we keep sensitive Blockchain key info in the back end protected and not exposed over communication between services. This database/layer will be hosted separately on each organization's premises and will be handled by the defined admin. Admins can create groups or assign roles/access to menus and services by an admin dashboard in UI. Access to Blockchain will be defined by roles and permissions decided in each jurisdiction. Blockchain roles can be in sync with identity manager roles or allocated in an appropriate way.

[At Iteration 4] The user and Identity management is a key function in LOCARD securing the application. It uses open protocol standards like OpenID Connect or SAML 2.0. The standalone server provides the option to create multiple realms, manage and configure them for multiple applications. The benefit of the authorization process followed is that the users are completely isolated from applications, and applications never see a user's credentials. After login, the server returns a token that is cryptographically signed, which can be used from the application to identify the user and authenticate.

SELP.V4.1.018	Please provide more information about the access rights, focusing on various roles in a criminal procedure, differences between levels of access and the requirements thereto.	Identity manager will have its own node and admin per jurisdiction. Here data access and flow are being handled by the bpm/portal first and then we will apply the same rules where needed in the identity Manager module. So, if there is a data access diagram per role you can attach it here.	Process needs to be standardized and recorded in the final user manual. Roles and responsibilities of the administrator should be defined in a comprehensive manner.	Each role defined so far in the system provides different functionalities and possibilities in the system (actually 3 main roles, plus the system administrator). These roles are properly defined in WP5 deliverables and mimic in a generic way current roles existing in forensic organisations and LEAs.	**Compliant**

Deviant Patterns Repository (ARC)

[At Iteration 3] This module consists of two main parts. Note that this module can act as a standalone system and therefore, its interaction with the system is now proposed as such. Nevertheless, the integration of this module inside LOCARD will be assessed during the implementation phase. We therefore elaborate a concise explanation of this module due to its specific features and sensitive data management procedures, since it is one of the key research points of LOCARD.

[At Iteration 4] The Deviant Patterns Repository module is implemented using a fault-tolerant, distributed architecture leveraging a distributed task queue for orchestrating and distributing the jobs to multiple workers, in order to ensure the timely monitoring and analysis of data from multiple sources, including social media and Social Live Streaming Services. At the user-produced data is collected, it is propagated to Grooming Detection and Explicit Imagery Detection submodules, for identifying patterns of predatory or criminal behaviours. Moreover, the ML models for these modules will allow re-training and fine tuning as new data becomes available, in order to enhance the detection accuracy of deviant patterns in novel data.

SELP.V4.1.021	Where is the repository physically located (during the project and after)?	In the LOCARD Server database that serves each end user node.	Follow-up question	During the project in the cloud of MOTIVIAN. After the project, it will depend on the deployment scenarios and the requirements of each organisation.	**Compliant**
SELP.V4.2.021	Will data be stored only locally? Will it be separated from other databases in terms of accessibility?	Concerning the use of the component local storage is used at ARC premises. In LOCARD the use of the component will be carried out by LEAs and storage will be local at their premises.	Details of data storage should be verified and further detailed by LEAs.	The repositories to be used and the deployment can be made either in local databases and servers or in the cloud. Hybrid capabilities have not been foreseen but the deployment of the LOCARD system components has some degrees of flexibilities. The answer depends on each organisation requirements.	**Compliant** - The organisations should be given handbooks or training materials in order to protect personal data on the cloud.
SELP.V4.1.022	Is it possible to use the other components of LOCARD (investigator's toolkit, storage manager, etc) together with this repository? How will it affect the use of the	The deviant behaviour will be integrated into the platform. The data used by the investigators during the project will be synthetic, and blockchain will only store hashes. All tools are independent and integrated under the evidence	It should be clarified what information is stored on the blockchain reference hashes data (contradiction with previous components - SELP.V3.1.017). A list of the data stored on the blockchain is essential.	The evidence is stored and used seamlessly by the tools.	**Compliant**

	system (with special attention to information sent to the blockchain and authorization)?	collected process that is built into the LOCARD platform. All inputs from all tools are considered evidence and are sent to the smart contract module.			
Questions newly added to Iteration 4					
Ref. number	Question	System module/Answer	Status - Recommendation		
SELP.V4.1.032	As the LOCARD system uses Blockchain technology and smart contract, does this technology poses any threat to the rights of the data subject?	Since data stored in blockchain are only hashes coming from combination of data, namely evidence files, metadata strings and so on, the issue of immutability is minimised. The security of this mechanism is tied to the irreversibility of hashes. Moreover, we use hashes over combination of data and never over a single datum (e.g. we do not hash a user identifier and store it in a single piece, but for instance multiple sources and combination of metadata from a case,	**Compliant** - Technical measures adapted to protect data subject's rights are appreciated.		

		timestamps etc), which increases the complexity and prevents the use of hashes as a pseudonymisation tool.	
SELP.V4.1.033	In a case where a data subject requires that his/her personal data stored/shown by the authority is not correct or needs to be rectified, can the authority (or investigator) do so by using the LOCARD system? Please take blockchain into consideration as well. If yes, can it be instantaneous or will it take time (and	It would take the time to modify and/or delete them from the system, which is similar to any related applications, namely in a matter of seconds. This is not tied to further checks, petitions, or protocol requirements subject to each specific jurisdiction, which fall out of the scope of LOCARD.	**Compliant**

	how much)?		
SELP.V4.1.034	What mechanisms will be used by the LOCARD system to rectify personal data?	LOCARD can modify data from individuals or delete it accordingly since these are stored in a database. As previously said, this is not tied to further checks, petitions, or protocol requirements subject to each specific jurisdiction, which fall out of the scope of LOCARD.	**Compliant**
SELP.V4.1.035	Taking into account the 'data minimisation' and 'purpose limitation' principles, is there any possibility that LOCARD system may store more data as it actually thought by the investigator?	Data stored and requested is the one needed strictly for the investigation purposes. The system is transparent to the investigation in this regard since each single piece of evidence is uniquely identified and can be checked and audited.	**Compliant**

SELP.V4.1.036	Is there any other way that the LOCARD system will use methods, such as on-chain and off-chain storage of personal data, in order to reach as close as possible to the data erasure?	LOCARD uses the storage datasets for the evidence and other data, and blockchain only for hashes (minimal on-chain information). Data are connected by unique IDs. This approach guarantees the use of the proper deletion mechanism and prevents the issue of storing personal data on-chain.	**Compliant**
SELP.V4.1.037	In a case where a court orders to transfer a piece of evidence (containing personal data) from the LOCARD system to other system(s) where no blockchain like platform is available, what would be the mechanisms then? Please	The mechanism will be precisely the same as currently used by LEAs or end-users to send evidence. This protocols are tied to each jurisdiction and out of the scope of LOCARD. LOCARD enables the flow of transferring an evidence, thus the evidence will appear as transferred in the system if required for the investigation purposes despite the other end point not having a LOCARD system.	**Compliant**

	also comment on the technicality involved and the time taken by the LOCARD system.	Further materials can be manually uploaded to complement the investigation and guarantee the full chain of custody, such as uploading manually e.g. a signed file related to the proper transfer of the case or an evidence to another end user.	
SELP.V4.1.039	Can the investigator/authority, using the LOCARD system, provide the data subject the information relating to him/her in a concise, transparent, intelligible, and easily accessible form by using clear and plain language? How much data can	This is in the crowdsource intelligence engine. All the information related to a user's rights and etc is shown there almost immediately.	**Compliant**

	the system need to perform this task?		
SELP.V4.1.040	What level of robustness and system security does the LOCARD platform guarantee against n and 0-order vulnerabilities?	The work being done is described in deliverable D6.5. This document provides a profound understanding of the security built into LOCARD.	**Compliant**

Table 7: Summary of SELP Continuous Monitoring

11 Annex 1: Assessment of Iteration 4

LOCARD

May 2022

SELP* Assessment Handbook

*Societal, Ethical, Legal and Privacy

V1.00

1

Contents

LOCARD

2

2

Introduction - 1

This document supplements the formal LOCARD deliverable D2.5 and is intended to be used by LOCARD partners as a guide to the performance and progress of the project against SELP best practice.

During the course of the LOCARD Project, continuous assessment has taken place and consisted of four iterations in order to ensure the monitoring of the dynamic process towards complete compliance. As such there may be some inconsistency between iterations due to the evolution in the LOCARD platform. These have been addressed as additional questions between iterations.

3

3

Introduction - 2

The questions aimed to identify the details of the functioning of the components, focusing on SELP considerations, with special attention to the processing of data. As questions address each component, partners responsible for the specific component were assigned with specific sets of questions individually in order to ensure that the answers are based on the required expertise and knowledge.

4

4

Explanation of Terms

This document forms a supplement to the LOCARD Social, Ethical, Legal and Privacy (SELP) impact assessment.

A result designated as **COMPLIANT** is considered to meet the LOCARD project SELP requirements.

A result designated as **NEUTRAL** is considered to be on track to meeting the LOCARD project SELP requirements by its first production release.

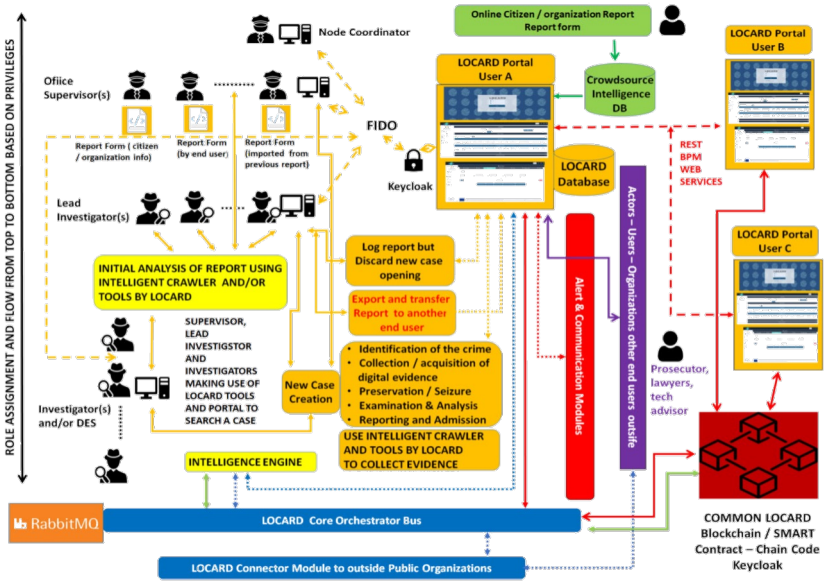
A result designated as **FAIL** is considered not to be able to meet the LOCARD project SELP requirements without a specific effort or has not yet been considered.

LOCARD

5

5

Release Candidate Architecture



LOCARD SELP Results Summary

6

6

LOCARD SELP Results Summary

Assessment results grouped by LOCARD Modules

7

7

LOCARD SELP Results Summary

LOCARD Module	Assessment Partner	
Intelligent Crawler	ICO	Infotrend Co. Ltd
Investigator's Toolkit	MOT	Motivian
Communication Engine	MOT	Motivian
Crowdsource Intelligence	MOT	Motivian
Storage Manager	NRS	Neurosoft
Blockchain Manager	NRS	Neurosoft
User and Identity Manager	NRS	Neurosoft
Intelligence Engine	IMC	IMC Technologies
Deviant Patterns Repository	ARC	Athena Innovation Centre
Connector	IMC	IMC Technologies
Reporting Engine	MOT	Motivian
Trusted Execution Environment	ARC	Athena Innovation Centre
LOCARD Portal	MOT	Motivian
GDPR Compliance Module (1)	VUB/MOT	Vrije Universiteit Brussel / Motivian
GDPR Compliance Module (2)	VUB/MOT	Vrije Universiteit Brussel / Motivian

LOCARD SELP Results Summary

8

8

Module : Intelligent Crawler

Assessment Partner : ICO

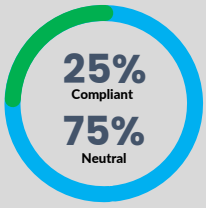
The Intelligent Crawler is an important module for searching the web. httrack website copier (www.httrack.com) is used which has many useful features like indexing a site according to the number of occurrences of a specific keyword indicating at the same time the page and the number of occurrences the keyword has been found within the page.

Iteration 4

Previous Assessment For Module (Iteration 3)

SELP:		
3.1.001	Where will the evidence storage be physically located? Is it the same repository as the Investigator's Toolkit and/or the Deviant Pattern Repository or after using the forensic tools, data will be either deleted or transferred to the evidence storage?	
3.1.002	Will the storage be tested with real data during the project?	
3.1.003	At what stage of the criminal procedure (and the use of LOCARD) is the data transferred to this repository? Until when is it kept there?	
3.2.003	Supplementary Question: Does the HTTrack mirrored site have any use once the content is copied to the investigator's toolkit	

Iteration 3



LOCARD SELP Results Summary

9

9

Module : Investigator's Toolkit

Assessment Partner : MOT

The investigator toolkit incorporates a set of forensic tools which have been developed by LOCARD University partners. There are three (3) broad categories of such tools, namely:

1. tools for streaming forensics
2. tools for cloud forensics
3. tools for mobile forensics

Iteration 4

Previous Assessment For Module (Iteration 3)

SELP:		
3.1.004	Will the forensic tools be used during the project on real data?	

Iteration 3

LOCARD SELP Results Summary

10

10

Module : Communication Engine

Assessment Partner : MOT

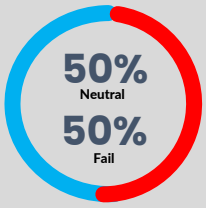
As required by many end users, the possibility of communication between LOCARD users is a desirable feature. To this end, LOCARD aims to allow investigators to publish some evidence, so that others can find similarities. In this case, the Communication Engine will allow them to exchange information, should they be given this permission, and log all the corresponding messages.

Iteration 4

Previous Assessment For Module (Iteration 3)

SELP:	
3.1.005	Where will the mails be physically stored (both during the project and in real life setting)? How will they be tamper-proof?
3.1.006	Can these emails be extracted to be used at the court?

Iteration 3



LOCARD SELP Results Summary

11

11

Module : Crowdsource Intelligence

Assessment Partner : MOT

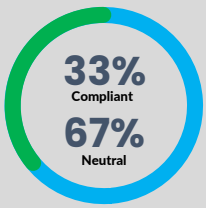
This module is about collecting digital crime incidents data reported from the general public / citizens and organizations, hence of great importance. To this end, citizens and organizations will be able to freely report content related to digital crime incidents.

Iteration 4

Previous Assessment For Module (Iteration 3)

SELP:	
3.1.007	What information is requested from the users during registration? Where is the user data stored and until when?
3.1.008	Do you have policies and info sheets in place for the users? Who can access the users' profile?
3.1.009	Do users have criminal liability when using the system (e.g. false accusation)?
3.1.010	If the exact details are outside the scope of the project (as stated in D3.5 p21), where are the actual boundaries thereof?
3.1.011	Is there any actual testing foreseen during the project? How do you ensure the adequacy and user-friendliness of the platform?
3.1.012	Where are the crowdsource intelligence, inputs stored?

Iteration 3



LOCARD SELP Results Summary

12

12

LOCARD SELP Results Summary

Module : Storage Manager

Assessment Partner : NRS

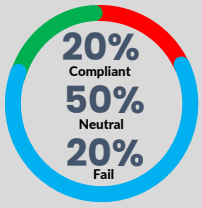
The storage manager provided is a distributed database which features high availability, consistency and scalability; acting as a supplementary role of a unifying distributed storage layer.

Iteration 4

Previous Assessment For Module (Iteration 3)

SELP:	
3.1.013	Where will the evidence storage be physically located? Is it the same repository as the Investigator's Toolkit and/or the Deviant Pattern Repository or after using the forensic tools, data will be either deleted or transferred to the evidence storage?
3.2.013	provide a further clarification on how the evidence storage works and what is its raison d'etre, as well as the categories of metadata to be used.
3.1.014	Will the storage be tested with real data during the project?
3.1.015	At what stage of the criminal procedure (and the use of LOCARD) is the data transferred to this repository? Until when is it kept there?
3.2.015	Provide further clarification regards to relationships to off-chain storage and blockchain information pointers.?

Iteration 3



13

13

LOCARD SELP Results Summary

Module : Blockchain Manager

Assessment Partner : NRS

The goal of the blockchain manager is threefold, namely:

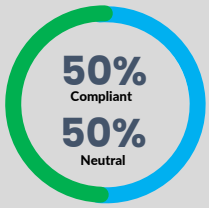
1. successfully create the blockchain network. The network will comprise nodes for each of the end users participating in the project.
2. to deploy the smart contract to the network which will provide much of the functionality for the LOCARD project.
3. to provide an API which will interact with the smart contract and which authorizes a user. Then this user will be able to interact with the blockchain network.

Iteration 4

Previous Assessment For Module (Iteration 3)

SELP:	
3.1.016	Who will overview the applicability and compliance of smart contracts during and after the project?
3.1.017	What type of data will be shared on the blockchain (as metadata)?

Iteration 3



14

14

Module : User and Identity Manager

Assessment Partner : NRS

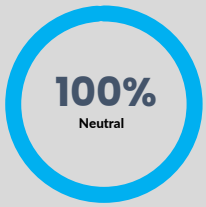
The User and Identity management is a key function in LOCARD securing the application. It uses open protocol standards like OpenID Connect or SAML 2.0. The standalone server provides the option to create multiple realms, manage and configure them for multiple applications. The benefit of the authorization process followed is that the users are completely isolated from applications and applications never see a user's credentials. After login, the server returns a token that is cryptographically signed, which can be used from the application to identify the user and authenticate.

Iteration 4

Previous Assessment For Module (Iteration 3)

SELP:	
3.1.018	Please provide more information about the access rights, focusing on various roles in a criminal procedure, differences between levels of access and the requirements thereto.

Iteration 3



LOCARD SELP Results Summary

15

15

Module : Intelligence Engine

Assessment Partner : IMC

The intelligence engine's main aim is to process the data existing in the context of LOCARD to provide intelligence and extract correlations to ease criminal investigation. Moreover, this data, after being retrieved and stored by the Intelligence Engine module, can potentially be used to query other external sources and well-known repositories outside LOCARD. This module is divided into several subcomponents and procedural flows as follows:

1. Data gathering
2. Data processing
3. Similarity computation
4. Query/Response

Iteration 4

Previous Assessment For Module (Iteration 3)

SELP:	
3.1.019	The intelligence engine will get access only to the blockchain or also to other databases, such as the Investigator's Toolkit, the Deviant Pattern Repository and the Evidence Storage?

Iteration 3

LOCARD SELP Results Summary

#1 16

16

Module : Deviant Patterns Repository

Assessment Partner : ARC

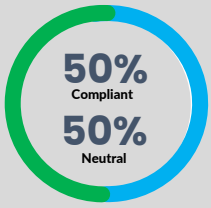
The Deviant Patterns Repository module is implemented using a fault-tolerant, distributed architecture leveraging a distributed task queue for orchestrating and distributing the jobs to multiple workers, in order to ensure the timely monitoring and analysis of data from multiple sources, including social media and Social Live Streaming Services. As the user-produced data is collected, it's propagated to Grooming Detection and Explicit Imagery Detection submodules, for identifying patterns of predatory or criminal behaviors. Moreover, the ML models for these modules will allow re-training and fine tuning as new data becomes available, in order to enhance the detection accuracy of deviant patterns in novel data.

Iteration 4

Previous Assessment For Module (Iteration 3)

SELP:	
3.1.020	Based on what will the deviant behaviour be defined and kept updated in the Deviant Patterns Repository in the project and afterwards? Is it possible to set any kind of behaviour as deviant?
3.2.020	Please provide more information and clarification about the functioning of the component. How does it carry out the evaluation? Who defines supervises the scoring system and based on what? .....
3.1.021	Where is the repository physically located (during the project and after)?
3.1.022	Is it possible to use the other components of LOCARD (investigator's toolkit, storage manager, etc) together with this repository? How will it affect the use of the system (with special attention to information sent to the blockchain and authorization)?

Iteration 3



LOCARD SELP Results Summary

17

17

Module : Connector

Assessment Partner : IMC

This module acts as the link between the LOCARD platform and external repositories. More concretely, the intelligence engine, which extracts and correlates information from the LOCARD platform and blockchain, will be also used to gather information from other sources by means of the connector. This way, more information can be used to correlate LOCARD cases with external investigations.

Iteration 4

Previous Assessment For Module (Iteration 3)

SELP:	
3.1.023	What type of information is expected to be imported to the LOCARD system?
3.2.023	Further information on compliance of external databases should be gathered to ensure cross-node information sharing (input from LEAs needed).
3.1.024	On what channels can evidence related be shared?
3.1.025	How will this component be tested during the project (i.e. with real or dummy data)?

Iteration 3

LOCARD SELP Results Summary

18

18

Module : Reporting Engine

Assessment Partner : MOT

This module is responsible for the presentation of information to the corresponding users and roles. On the one hand, it is in charge of (a) aggregating information for specific documents targeted to specific roles, which occurs as soon as the Intelligence Engine finds tangible correlations and prioritizes them, and (b) keeping track of the chain of custody and digital evidence. On the other hand, it has the task of providing management with meaningful input to the corresponding authorities such as LEAs, Forensics Labs, Corporate Organizations.

Iteration 4

Previous Assessment For Module (Iteration 3)

SELP:		
3.1.026	Will the report queries be logged?	
3.1.027	Can a LOCARD user access the evidence related data through the reporting engine or other services of the system?	
3.2.027	Who will specify the admin person per each organization? We need to list and elaborate on the compliance process.	

Iteration 3

LOCARD SELP Results Summary

19

19

Module : Trusted Execution Environment

Assessment Partner : ARC

Most web applications rely their authentication process on the password paradigm. It is evident that a password can be considered secure when it contains 20 characters or more, is complex (is composed of alphanumeric, symbols and non-dictionary words), is only stored in the brain of the user, is used only in one application and is changed frequently.

In this context, the need to employ a secure and user-friendly password-less authentication solution has emerged. FIDO (Fast Identity Online) proposes a strong authentication scheme in which the user is authenticated to the device deploying built-in platform authenticators or capabilities fingerprint sensors, cameras, microphones, embedded TPM hardware), and the latter is authenticated to the server using a challenge-response scheme and public key cryptography. The benefits of this method are:

- User credentials are now stored on the user's device in a trusted environment.
- Server only stores the public key of the user authentication process.
- Users do not have to remember complex passwords (convenience & security).
- Users can select the authentication mechanism of their preference (PIN, biometrics, etc.) and use it for different services.
- Authentication keys are different for different services.
- FIDO protocol can be combined with existing technologies and it is highly extensible.
- Both the server and the client are protected.

Iteration 4

Previous Assessment For Module (Iteration 3)

SELP:		
3.1.028	Please explain why it is necessary to have a separate platform in parallel with LOCARD.	
3.1.029	How does the use of TEE affect the LOCARD smart contracts, authorization rights, data transfers, blockchain info, etc.?	

Iteration 3

LOCARD SELP Results Summary

20

20

Module : LOCARD Portal

Assessment Partner : MOT

The LOCARD portal integrates the different modules of the LOCARD system, each with its corresponding internal databases and policies. In general, data crawled from external sources is stored in the corresponding protected database (according the local policies). This operation, as well as the identity management interactions, are executed in a trusted environment context. Next, the data stored, namely digital evidence, will be processed and analysed (where applicable) by the investigator toolkit, which contains several forensic tools. Consequently, a report will be generated in each case, which will be used to update the investigator(s) involved in the case by using the alert engine.

Iteration 4

Previous Assessment For Module (Iteration 3)

SELP:	
3.1.030	How do you aim to address the level of acceptability of the portal (difficulty of use, fixing potential bugs, feature, and GUI updates, etc.)?

Iteration 3

LOCARD SELP Results Summary

21

21

Module : GDPR Compliance (New module) – Part 1

Assessment Partner : VUB/MOT

This is a general assessment as to the compliance of LOCARD as it is intended to be used in operations. LOCARD is part of the process for collection and recording digital crime incidents data and reports from the general public/citizens and Law Enforcement Investigation organizations, and whilst much is exempt from GDPR restrictions, being part of those criminal investigations, the issue is still of great importance in the case of this not being the case.

Iteration 4

Assessment For Module (Introduced in Iteration 4)

SELP:	
4.1.031	Does the LOCARD system respects the data subject's rights under the GDPR, in general? (Please explain response)
4.1.032	As the LOCARD system uses Blockchain technology and smart contract, does this technology poses any threat to the rights of the data subject?
4.2.032	Please comment on the particular rights that can be challenged because of the nature and characteristics of the technology. Please also comment on the degree of threat.
4.1.033	In a case where a data subject requires that his/her personal data stored/shown by the authority is not correct or needs to be rectified, can the authority (or investigator) do so by using the LOCARD system, please take Blockchain into consideration as well? If yes, can it be instantaneous, or will it take time (and how much)?
4.1.034	What mechanisms will be used by the LOCARD system to rectify personal data?
4.1.035	Taking into account the 'data minimisation' and 'purpose limitation' principles, is there any possibility that LOCARD system may store more data as it actually thought by the investigator?
4.1.036	Is there any other way that the LOCARD system will use methods, such as on-chain and off-chain storage of personal data, in order to reach as close as possible to the data erasure?

Iteration 4

LOCARD SELP Results Summary

22

22

Module : GDPR Compliance (New module) – Part 2

Assessment Partner : VUB/MOT

This is a general assessment as to the compliance of LOCARD as it is intended to be used in operations. LOCARD is part of the process for collection and recording digital crime incidents data and reports from the general public/citizens and Law Enforcement Investigation organizations, and whilst much is exempt from GDPR restrictions, being part of those criminal investigations, the issue is still of great importance in the case of this not being the case.

Iteration 4

Assessment For Module (Introduced in Iteration 4)

SELP:		
4.1.037	In a case where a court orders to transfer a piece of evidence (containing personal data) from the LOCARD system to other system(s) where no Blockchain like platform is available, what would be the mechanisms then? Please also comment here on the technicality involved and the time taken by the LOCARD system.	
4.1.038	In a case where a court orders to transfer a piece of evidence (containing personal data) from the LOCARD system to other system(s) where a Blockchain like platform is available, what would be mechanisms then? Please also comment here on the technicality involved and the time taken by the LOCARD system.	
4.1.039	Can the investigator/authority, using the LOCARD system, provide the data subject the information relating to him/her in a concise, transparent, intelligible, and easily accessible form by using clear and plain language? How much time can the system need to perform this task?.	
4.1.040	What level of robustness and system security does the LOCARD platform guarantee against n and 0-order vulnerabilities?	

Iteration 4

LOCARD SELP Results Summary

23

23

LOCARD Final Results Details

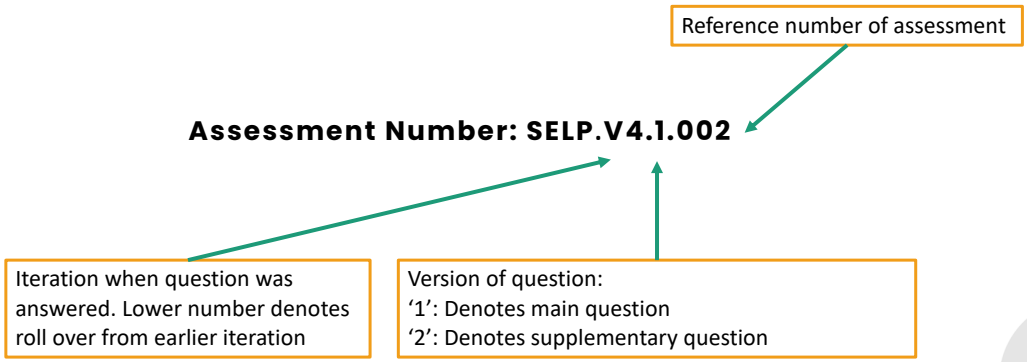
Assessment results in full

Note that numbering of assessments indicates when the assessment was last asked.

24

24

Numbering of Assessments



25

25

Index of Assessments

Assessment Number	Assessment Description
V3.1.001	Where is the mirrored website by HTTRack physically stored during the project and in real life setting? Is the update automatic or manual? Only the html is mirrored or the content (videos, audio, other files) as well?
V4.1.002	When will the mirrored website be deleted? Is it automatic or manual deletion? Who is responsible for the deletion mechanism?
V4.1.003	The mirrored website or parts thereof will be copied to the Investigator's Toolkit and/or the Deviant Pattern Repository and the HTTrack will delete the mirror. Does this deletion depends only on the fact of the copy?
V4.2.003	Supplementary Question: Does the HTTrack mirrored site have any use once the content is copied to the investigator's toolkit?
V4.1.004	Will the forensic tools be used during the project on real data?
V4.1.005	Where will the mails be physically stored (both during the project and in real life setting)? How will they be tamper-proof?
V4.1.006	Can these emails be extracted to be used at the court?
V4.1.007	What information is requested from the users during registration? Where is the user data stored and until when?
V4.2.007	How will authentication occur? What are the details of the data storage (time, reason, connection with other database, etc.) The information stored in the LEAs' system is separated from other databases?
V4.1.008	Do you have policies and info sheets in place for the users? Who can access the users' profile?
V4.1.009	Do users have criminal liability when using the system (e.g. false accusation)?
V4.1.010	If the exact details are outside the scope of the project (as stated in D3.5 p21), where are the actual boundaries thereof?

26

26

Index of Assessments

Assessment Number	Assessment Description
V4.1.011	Is there any actual testing foreseen during the project? How do you ensure the adequacy and user-friendliness of the platform?
V3.1.012	Where are the crowdsource intelligence, inputs stored? We need more visibility and a formal process (Perhaps stamps who has executed the change; Audit trail etc
V4.1.013	Where will the evidence storage be physically located? Is it the same repository as the Investigator's Toolkit and/or the Deviant Pattern Repository or after using the forensic tools, data will be either deleted or transferred to the evidence storage?
V4.1.014	Will the storage be tested with real data during the project?
V4.1.015	At what stage of the criminal procedure (and the use of LOCARD) is the data transferred to this repository? Until when is it kept there?
V4.2.015	Please provide a further clarification in regard to relationships to off-chain storage and blockchain information pointers.?
V4.1.016	Who will overview the applicability and compliance of smart contracts during and after the project?
V3.1.017	What type of data will be shared on the blockchain (as metadata)?
V4.1.018	Please provide more information about the access rights, focusing on various roles in a criminal procedure, differences between levels of access and the requirements thereto.
V3.1.019	The intelligence engine will get access only to the blockchain or also to other databases, such as the Investigator's Toolkit, the Deviant Pattern Repository and the Evidence Storage?
V3.1.020	Based on what will the deviant behaviour be defined and kept updated in the Deviant Patterns Repository in the project and afterwards? Is it possible to set any kind of behaviour as deviant?
V3.2.020	Please provide more information and clarification about the functioning of the component. How does it carry out the evaluation? Who defines supervises the scoring system and based on what? Will the scoring system be general or jurisdiction specific? How will potential differences affect the applicability of the component in an international environment/case?

27

27

Index of Assessments

Assessment Number	Assessment Description
V4.1.021	Where is the repository physically located (during the project and after)?
V4.2.021	Will data will be stored only locally? Will it be separated from other databases in terms of accessibility?
V4.1.022	Is it possible to use the other components of LOCARD (investigator's toolkit, storage manager, etc) together with this repository? How will it affect the use of the system (with special attention to information sent to the blockchain and authorization)?
V3.1.023	What type of information is expected to be imported to the LOCARD system?
V3.2.023	Further information on compliance of external databases should be gathered to ensure cross-node information sharing (input from LEAs needed).
V3.1.024	On what channels can evidence related be shared and who has authorization to share information?
V3.1.025	How will this component be tested during the project (i.e. with real or dummy data)?
V3.1.026	Will the report queries be logged?
V3.1.027	Can a LOCARD user access the evidence related data through the reporting engine or other services of the system?
V3.2.027	Who will specify the admin person per each organization? We need to list and elaborate on the compliance process.
V3.1.028	Please explain why it is necessary to have a separate platform in parallel with LOCARD.
V3.1.029	How does the use of TEE affect the LOCARD smart contracts, authorization rights, data transfers, blockchain info, etc.? Can we have a statement of usability of the components? Can we ensure the same level of security?

28

28

Index of Assessments

Assessment Number	Assessment Description
V3.1.030	How do you aim to address the level of acceptability of the portal (difficulty of use, fixing potential bugs, feature, and GUI updates, etc.)?
V4.1.032	As the LOCARD system uses Blockchain technology and smart contract, does this technology poses any threat to the rights of the data subject?
V4.1.033	In a case where a data subject requires that his/her personal data stored/shown by the authority is not correct or needs to be rectified, can the authority (or investigator) do so by using the LOCARD system, please take Blockchain into consideration as well? If yes, can it be instantaneous, or will it take time (and how much)?
V4.1.034	What mechanisms will be used by the LOCARD system to rectify personal data?
V4.1.035	Taking into account the 'data minimisation' and 'purpose limitation' principles, is there any possibility that LOCARD system may store more data as it actually thought by the investigator?
V4.1.036	Is there any other way that the LOCARD system will use methods, such as on-chain and off-chain storage of personal data, in order to reach as close as possible to the data erasure?
V4.1.037	In a case where a court orders to transfer a piece of evidence (containing personal data) from the LOCARD system to other system(s) where **no Blockchain like platform is available**, what would be the mechanisms then? Please also comment here on the technicality involved and the time taken by the LOCARD system.
V4.1.038	In a case where a court orders to transfer a piece of evidence (containing personal data) from the LOCARD system to other system(s) where **a Blockchain like platform is available**, what would be mechanisms then? Please also comment here on the technicality involved and the time taken by the LOCARD system.
V4.1.039	Can the investigator/authority, using the LOCARD system, provide the data subject the information relating to him/her in a concise, transparent, intelligible, and easily accessible form by using clear and plain language? How much time can the system need to perform this task?.
V4.1.040	What level of robustness and system security does the LOCARD platform guarantee against in and 0-order vulnerabilities?

29

29

Assessment Number: SELP.V3.1.001

Assessment Description

Where is the mirrored website by HTTRack physically stored during the project and in real life setting? Is the update automatic or manual? Only the html is mirrored or the content (videos, audio, other files) as well?

Response

The user chooses the physical location where the mirror site will be stored by means of an input screen. That practically means that the user can store the site either locally or to a network drive manually at the respective LOCARD node. All files that comprise the site will be saved (audio , video etc).

Compliant

Recommendation

The user should be provided with options compliant with EU data protection law. This includes the location of data, which should be preferably within the EU. The details of storage should be always clear, transparent and traceable.

In LOCARD such options should be clarified and tested. This aspect should form part of the manual (Deliverable 5.5 Release candidate and associated manual and Deliverable 5.6 Final Release and associated manual), explaining the entire procedure of deployment and responsibilities.

LOCARD SELP Results Details

30

30

Assessment Number: SELP.V4.1.002

Assessment Description

When will the mirrored website be deleted? Is it automatic or manual deletion? Who is responsible for the deletion mechanism?

Response

Compliant

The deletion of an evidence is managed by the investigator(s) if applicable. It will follow the same procedure than evidence, once in a case it can only be deleted or erased in some specific occasions, mostly at the end of a case. A mirrored website, from the moment it is collected in the context of a case and thus becomes an evidence, is no exception.

Recommendation

It is advised to adopt a plan that clearly figures out the responsibilities of the investigator(s) regarding management of mirrored website, including data deletion. The plan should include policies equally applicable to all investigators, throughout the LOCARD system. There should not be any fix policy that the mirrored website can only be deleted at the end of some specific cases. Once the purpose of the data collection is met, the website should be deleted without undue delay. Automatic deletion mechanisms should be adopted and worked upon to make the LOCARD system robust.

LOCARD SELP Results Details

31

31

Assessment Number: SELP.V4.1.003

Assessment Description

The mirrored website or parts thereof will be copied to the Investigator's Toolkit and/or the Deviant Pattern Repository and the HTTrack will delete the mirror. Does this deletion depends only on the fact of the copy?

Response

Compliant

The data mirrored will be stored as evidence and it will be analysed either via the LOCARD platform or locally by the investigator..

The platform works in a simpler fashion. The website is mirrored and stored as evidence. If a URL is queried from the deviant behavior the functionality is the same.

Recommendation

Whoever will be responsible for the analysis and whatever will be the mode of that analysis, deletion must be ensured. A guideline should be made available to the investigator(s) about which mode of analysis, either through the LOCARD platform or locally, will provide greater legal compliance.

LOCARD SELP Results Details

32

32

Assessment Number: SELP.V4.2.003

Assessment Description

Supplementary Question: Does the HTTrack mirrored site have any use once the content is copied to the investigator's toolkit?

Response

Compliant

If there exists a copy in the evidence dataset, any temporary files can be dismissed. Thus, it can be later used and analysed accordingly.

Recommendation

A data retention policy should be defined.

LOCARD SELP Results Details

33

33

Assessment Number: SELP.V4.1.004

Assessment Description

Will the forensic tools be used during the project on real data?

Response

Compliant

No real data will be used. This is stated in the Data Management Plan of the project as well.

Recommendation

Any change in this plan should be discussed first and assessed according to the SELP benchmarks.

LOCARD SELP Results Details

34

34

Assessment Number: SELP.V4.1.005

Assessment Description

Where will the mails be physically stored (both during the project and in real life setting)? How will they be tamper-proof?

Response

The mails if they are collected as an evidence during an investigation have the same applicability than any evidence. About the communication between investigators, since the chat is for general purpose, nothing is logged as any evidence in any specific case. Note that the information could refer to distinct cases in the chat. The internal communication has a similar purpose that other messaging systems such as Skype, but it is executed inside of the platform for security and privacy reasons. However, the investigators, if desired, could manually create a transcript of any specific part and upload it as a new document in the case

Compliant

Recommendation

Similar protection should be provided to the emails as well that contain general-purpose chats. In a case where email chat can be used in court, it becomes necessary to protect it from tampering since its inception. A mechanism must be adopted to protect emails from tampering. The recommendation provided in the previous version i.e., Iteration 3 (SELP.V3.1.005) is further emphasized.

LOCARD SELP Results Details

35

35

Assessment Number: SELP.V4.1.006

Assessment Description

Can these emails be extracted to be used at the court?

Response

Please, refer to the previous question. Depending on their scope. If these are introduced as evidence in the system, the procedure to do so will follow whatever procedure the current investigators follow (e.g. creating a certified copy, requesting further details to the email provider, etc).

Compliant

Recommendation

It is advised that email chats should also be added to the smart contract.

LOCARD SELP Results Details

36

36

Assessment Number: SELP.V4.1.007

Assessment Description

What information is requested from the users during registration? Where is the user data stored and until when?

Response

Compliant

This is detailed in the Deliverables where the Crowdsource engine is described. Data are stored during the scope of an investigation if needed, applying the same policies than current organisations would apply. The decision is not forced or limited by LOCARD, and relies on the owners of such data, which will be the recipients of the petition, namely each organisation(s). When deployed, each organisation will manage this details, LOCARD does not force or impose a policy.

Recommendation

The approach adopted by the LOCARD system policy in this regard is appreciated.

LOCARD SELP Results Details

37

37

Assessment Number: SELP.V4.2.007

Assessment Description

How will authentication occur? What are the details of the data storage (time, reason, connection with other database, etc.) The information stored in the LEAs' system is separated from other databases?

Response

Compliant

For internal users: registration is taking place on the platform with Keycloak through integration and also this is done because these users are authenticated to access the blockchain as well

For external users: no registration occurs. Information is stored on MariaDB. External individuals can submit information to LOCARD LEA partners as well as to TID or NRS.

Recommendation

Registration processes (or the lack thereof) should be described in the user manual.

LOCARD SELP Results Details

38

38

Assessment Number: SELP.V4.1.008

Assessment Description

Do you have policies and info sheets in place for the users? Who can access the users' profile?

Response

Dependent on users . Citizens - The crowdsource engine offers the same capabilities than typical LEAs or similar when collecting information. User's profiles and data facilitated during the process will be accessed by whoever is in charge of such a petition and thereafter a possible investigation. User's have their right to be deleted from the system applying GDPR policies, yet if they are part of an investigation and some data is relevant to it, it will remain according to the investigation needs. This will be assessed by the corresponding organisation. The LOCARD blockchain itself, only stores referenced hashes.

Compliant

Recommendation

Compliant

LOCARD SELP Results Details

39

39

Assessment Number: SELP.V4.1.009

Assessment Description

Do users have criminal liability when using the system (e.g. false accusation)?

Response

This is out of the scope of LOCARD. The corresponding laws will apply according to each jurisdiction . This reflects T&Cs in the non-automated chain of custody currently in use. To be addressed by future users of the LOCARD platform if desired. To be mentioned in the user manual.

Compliant

Recommendation

The LOCARD system user manual must incorporate policies regarding criminal liability for the users in the case when a false accusation is made by the user itself or when the user allows such accusations to the system knowingly. A clarification on this account should be provided in the user manual.

LOCARD SELP Results Details

40

40

Assessment Number: SELP.V4.1.010

Assessment Description

If the exact details are outside the scope of the project (as stated in D3.5 p21), where are the actual boundaries thereof?

Response

Compliant

Similar to the previous question. It is out of scope. There have not been discussions towards this, which would entail assessing them in any post-LOCARD governance discussions

Recommendation

Compliant

LOCARD SELP Results Details

41

41

Assessment Number: SELP.V4.1.011

Assessment Description

Is there any actual testing foreseen during the project? How do you ensure the adequacy and user-friendliness of the platform?

Response

Compliant

There are several testing activities, as part of WP6. The UI/UX have been designed according to several well-known development mechanisms. These details are stated in the different deliverables of WP5, and in the Architecture deliverable D3.5

Recommendation

Requirements met (as recommended in Iteration 3).

LOCARD SELP Results Details

42

42

Assessment Number: SELP.V3.1.012

Assessment Description

Where are the crowdsource intelligence, inputs stored? We need more visibility and a formal process (Perhaps stamps who has executed the change; Audit trail etc

Response

Compliant

On the MariaDB database of the LOCARD platform. The data is physically stored on the LOCARD servers on the cloud, in a secure data center in Germany. Details of the storage should be clarified. We need more visibility and a formal process (Perhaps stamps who has executed the change; Audit trail etc). If a future user wants to have every information on a local server – consortium should give the technical requirements to set up with the necessary security measures

Recommendation

Compliant

LOCARD SELP Results Details

43

43

Assessment Number: SELP.V4.1.013

Assessment Description

Where will the evidence storage be physically located? Is it the same repository as the Investigator's Toolkit and/or the Deviant Pattern Repository or after using the forensic tools, data will be either deleted or transferred to the evidence storage?

Response

Compliant

Data are stored according to each organisation's needs, either on premise as part of their current databases, or in the cloud. The system uses such storage datasets for all the LOCARD platform, and data are fed into each component seamlessly to create the corresponding analysis and reports.

Recommendation

Compliant

LOCARD SELP Results Details

44

44

Assessment Number: SELP.V3.2.013

Assessment Description

Please provide a further clarification on how the evidence storage works and what is its raison d'etre, as well as the categories of metadata to be used.

Response

Compliant

The storage is on the LOCARD servers, in the dedicated module (SM). Further information to be found in D3.5 Reference Architecture.

Recommendation

Compliant

LOCARD SELP Results Details

45

45

Assessment Number: SELP.V4.1.014

Assessment Description

Will the storage be tested with real data during the project?

Response

Compliant

No. No personal data nor data coming from any real investigation will be used.

Recommendation

Compliant

LOCARD SELP Results Details

46

46

Assessment Number: SELP.V4.1.015

Assessment Description

At what stage of the criminal procedure (and the use of LOCARD) is the data transferred to this repository? Until when is it kept there?

Response

Compliant

As each step is logged into the blockchain contemporarily, , any modification or deletion of an evidence, regardless of their relevance, will be audited.

Recommendation

The Audit mechanism adopted to keep the system legally compliant is highly appreciated. However, a pre-audit and pre-modification/deletion stages policy should also be adapted to provide real-time protection to the rights of the data subject, for ex. 'right to rectification', 'right to erasure', etc.

LOCARD SELP Results Details

47

47

Assessment Number: SELP.V4.2.015

Assessment Description

Please provide a further clarification in regard to relationships to off-chain storage and blockchain information pointers.?

Response

Compliant

The Blockchain stores hashes in a tamper-proof manner, which are later used by other components of the platform. This way, auditability and verifiability are ensured. Other data stored in the transactions, such as investigator ID and use case ID can be used to further locate and ease reporting and audits.

Recommendation

Compliant

LOCARD SELP Results Details

48

48

Assessment Number: SELP.V4.1.016

Assessment Description

Who will overview the applicability and compliance of smart contracts during and after the project?

Response

Compliant

It will depend on each jurisdiction and what organisations will be part of the whole ecosystem. This would entail assessing them in any post-LOCARD governance discussions.

Recommendation

The LOCARD governance model should devise a plan wherein the responsibilities are clearly demarcated against the authority, for ex. DPA in a jurisdiction.

LOCARD SELP Results Details

49

Assessment Number: SELP.V3.1.017

Assessment Description

What type of data will be shared on the blockchain (as metadata)?

Response

Compliant

Since Blockchain by its nature ensures the immutability of data, hashes and metadata from evidence or tools can be stored there each time those are gathered. Not any data. Just hashes and metadata. Note. This does not include actual evidence

Recommendation

Compliant

LOCARD SELP Results Details

50

Assessment Number: SELP.V4.1.018

Assessment Description

Please provide more information about the access rights, focusing on various roles in a criminal procedure, differences between levels of access and the requirements thereto.

Response

Each role defined so far in the system provides different functionalities and possibilities in the system (actually 3 main roles, plus the system administrator). These roles are properly defined in WP5 deliverables and mimic in a generic way current roles existing in forensic organisations and LEAs.

Compliant

Recommendation

Compliant

LOCARD SELP Results Details

51

51

Assessment Number: SELP.V3.1.019

Assessment Description

The intelligence engine will get access only to the blockchain or also to other databases, such as the Investigator's Toolkit, the Deviant Pattern Repository and the Evidence Storage?

Response

The searchable fields are confirmed to be mainly hashes and so do not present any breach or threat.

Compliant

Recommendation

The metadata will be hashes (simplest form). IMC: we may extract other metadata and also do a search in that regard. I believe that this is directly related to the information stored in the blockchain, so we have to see the smart contracts, what information they store (hash, timestamp…) and these will be the potentially searchable fields. A simplistic description of the Intelligence engine operation: Evidence Creation messages send from Investigator's Toolkit, the Deviant Pattern Repository or the Evidence Storage to the Portal. The intelligence engine is listening to the evidence creation messages reported to the Portal (from the Orchestrator).

LOCARD SELP Results Details

52

52

Assessment Number: SELP.V3.1.020

LOCARD SELP Results Details

Assessment Description

Based on what will the deviant behaviour be defined and kept updated in the Deviant Patterns Repository in the project and afterwards? Is it possible to set any kind of behaviour as deviant?

Response

Compliant

The outcome of the deviant behaviour is a confidence score which states the degree of a content being deviant. The investigators can always have a second opinion, as always automated solutions need to be supervised. The interpretability of the results is done by the researcher and thus, the deviant behaviour provides an initial assessment based on the state-of-the-art knowledge

Recommendation

See supplementary question SELP v3.2.020

53

53

Assessment Number: SELP.V3.2.020

LOCARD SELP Results Details

Assessment Description

Please provide more information and clarification about the functioning of the component. How does it carry out the evaluation? Who defines supervises the scoring system and based on what? Will the scoring system be general or jurisdiction specific? How will potential differences affect the applicability of the component in an international environment/case?

Response

Compliant

Requested information can be found in deliverables D3.5, D5.2 and D5.3. Concerning the evaluation details: well-known benchmarks and metrics will be used (according to the defined KPIs), description will be included in D6.1. Validity of the confidence score in different jurisdictions is out of the scope of the component.

Recommendation

Scoring system should be validated throughout the validation activities. Decision-making based on the scores should be left to the organization

54

54

Assessment Number: SELP.V4.1.021

Assessment Description

Where is the repository physically located (during the project and after)?

Response

Compliant

During the project in the cloud servers managed by MOTIVIAN. After the project, will depend on the deployment scenarios and the requirements of each organisation.

Recommendation

Compliant

LOCARD SELP Results Details

55

55

Assessment Number: SELP.V4.2.021

Assessment Description

Will data will be stored only locally? Will it be separated from other databases in terms of accessibility?

Response

Compliant

The repositories to be used and the deployment can be made either locally in local databases and servers or in the cloud. Hybrid capabilities have not been foreseen but the deployment of the LOCARD system components has some degrees of flexibility. The answer is depending on each organisation requirements. Details of data storage should be verified and further detailed by LEAs

Recommendation

The organisations should be given handbooks or training materials in order to protect personal data on the cloud.

LOCARD SELP Results Details

56

56

Assessment Number: SELP.V4.1.022

LOCARD SELP Results Details

Assessment Description

Is it possible to use the other components of LOCARD (investigator's toolkit, storage manager, etc) together with this repository? How will it affect the use of the system (with special attention to information sent to the blockchain and authorization)?

Response

Compliant

Recommendation

Compliant

The evidence is stored

57

57

Assessment Number: SELP.V3.1.023

LOCARD SELP Results Details

Assessment Description

What type of information is expected to be imported to the LOCARD system?

Response

Compliant

Information from third party databases outside LOCARD like eg. Europol.

Recommendation

See supplementary question SELP v3.2.023

58

58

Assessment Number: SELP.V3.2.023

Assessment Description

Further information on compliance of external databases should be gathered to ensure cross-node information sharing (input from LEAs needed).

Response

Compliant

Out of scope of the project. Details to be defined by future users of the platform.

Recommendation

Details to be defined by future users of the platform.

LOCARD SELP Results Details

59

59

Assessment Number: SELP.V3.1.024

Assessment Description

On what channels can evidence related be shared and who has authorization to share information?

Response

Compliant

It will interact with the portal and the evidence screen in the system through RabbitMQ service bus . Authorization depends on the user profile. Connector is not yet implemented – not a problem for testing and validation (outside the scope of the project). Extracts from the smart contract can be shared

Recommendation

It will interact with the portal and the evidence screen in the system through RabbitMQ service bus . Authorization depends on the user profile. Although it is deemed outside of the project, based on discussions with partners it might become part of it later.

LOCARD SELP Results Details

60

60

Assessment Number: SELP.V3.1.025

Assessment Description

How will this component be tested during the project (i.e. with real or dummy data)?

Response

Compliant

So far we know that we will use dummy data. This whole process needs to be further analyzed in WP6 testing protocols to be specified. Can be tested internally through the API (not planned but can be tested).

Recommendation

Although it is deemed outside of the project, based on discussions with partners it might become part of it later. Should that happen, relevant partners should be notified.

LOCARD SELP Results Details

61

61

Assessment Number: SELP.V3.1.026

Assessment Description

Will the report queries be logged?

Response

Compliant

Yes. And there will be a reporting module that registered users can view.

Recommendation

Compliant

LOCARD SELP Results Details

62

62

Assessment Number: SELP.V3.1.027

LOCARD SELP Results Details

Assessment Description

Can a LOCARD user access the evidence related data through the reporting engine or other services of the system?

Response

Compliant

Yes, according to privileges provided by the admin responsible person in each organization.

Recommendation

No recommendation if the admin is dealing with the access rights .
See supplementary question SELP v3.2.027.

63

63

Assessment Number: SELP.V3.2.027

LOCARD SELP Results Details

Assessment Description

Who will specify the admin person per each organization? We need to list and elaborate on the compliance process.

Response

Compliant

Admin person is called 'node coordinator' – one or more user role in each organization. There will be in the long-term deployment an area coordinator – e.g. to add a new organization offline to the platform and to validate the new organization as well as the node coordinator and keep the directory of IDs. The Area coordinator could be LEA, ministry, depends. The testing of the component is not in the scope of the project but planned regarding governance. These roles and responsibilities should be clearly defined in the user manual

Recommendation

These roles and responsibilities should be clearly defined in the user manual.

64

64

Assessment Number: SELP.V3.1.028

Assessment Description

Please explain why it is necessary to have a separate platform in parallel with LOCARD.

Response

Compliant

TEE is not a platform outside of LOCARD. TEE is a module offered by modern processors and operating systems to ensure that a small set of operations (they do not support everything) will be performed in an isolated environment that cannot be manipulated externally. This is very critical in e.g. authentication in untrusted environments (consider the case of collecting digital evidence in a compromised device and you have to enter some credentials). Therefore, a TEE module is used in the LOCARD platform to ensure that critical components and actions are performed in a secure and isolated manner, providing protection to e.g. tampering, eavesdropping and etc. The use of a TEE will ensure the integrity of cryptographic operations which are used to produce signatures or key creation processes. Moreover, the storage of several components can be realised also in a TEE, in order to prevent external intrusion and guaranteeing the integrity of such system components.

Recommendation

Compliant

LOCARD SELP Results Details

65

65

Assessment Number: SELP.V3.1.029

Assessment Description

How does the use of TEE affect the LOCARD smart contracts, authorization rights, data transfers, blockchain info, etc.? Can we have a statement of usability of the components? Can we ensure the same level of security?

Response

Compliant

It doesn't affect them dire*ctly, but only providing* further security. Information is listed in D3.5 p39). Necessary information has been provided, no further request or recommendation.

Recommendation

Compliant

LOCARD SELP Results Details

66

66

Assessment Number: SELP.V3.1.030

Assessment Description

How do you aim to address the level of acceptability of the portal (difficulty of use, fixing potential bugs, feature, and GUI updates, etc.)?

Response

Compliant

We have a quality assurance team in place which will monitor, test and get feedback provided and will closely liaise with the technical team. we plan extensive seminars to teach operation of the platform and tools to the end users, development of user manual and PowerPoint presentations to guide them through the usage of the platform and tools as well as the functioning of the blockchain/smart contracts..

Recommendation

Compliant

LOCARD SELP Results Details

67

67

Assessment Number: SELP.V4.1.032

Assessment Description

As the LOCARD system uses Blockchain technology and smart contract, does this technology poses any threat to the rights of the data subject?

Response

Compliant

Since data stored in blockchain are only hashes coming from combinations of data, namely evidence files, metadata strings and so on, the issue of immutability is minimised. The security of this mechanism is tied to the irreversability of hashes. Moreover, we use hashes over combinations of data and never over a single datum (e.g. we do not hash a user identifier and store it a a single piece, but for instance multiple sources and combinations of metadata from a case, timestamps etc), which increases the complexity and prevents the use of hashes as a pseudonimization tool.

Recommendation

Technical measures adapted to protect data subject's rights are appreciated.

LOCARD SELP Results Details

68

68

Assessment Number: SELP.V4.1.033

LOCARD SELP Results Details

Assessment Description

In a case where a data subject requires that his/her personal data stored/shown by the authority is not correct or needs to be rectified, can the authority (or investigator) do so by using the LOCARD system, please take Blockchain into consideration as well? If yes, can it be instantaneous, or will it take time (and how much)?

Response

Compliant

It would take the time to modify and/or delete them from the system, which is similar to any related applications, namely in a matter of seconds. This is not tied to further checks, petitions, or protocol requirements subject to each specific jurisdiction, which fall out of the scope of LOCARD.

Recommendation

Compliant

69

69

Assessment Number: SELP.V4.1.034

LOCARD SELP Results Details

Assessment Description

What mechanisms will be used by the LOCARD system to rectify personal data?

Response

Compliant

LOCARD can modify data from individuals or delete it accordingly since these are stored in a database. As previously said, this is not tied to further checks, petitions, or protocol requirements subject to each specific jurisdiction, which fall out of the scope of LOCARD.

Recommendation

Compliant

70

70

Assessment Number: SELP.V4.1.035

Assessment Description

Taking into account the 'data minimisation' and 'purpose limitation' principles, is there any possibility that LOCARD system may store more data as it actually thought by the investigator?

Response

Compliant

Data stored and requested is the one needed strictly for the investigation purposes. The system is transparent to the investigators in this regard since each single piece of evidence is uniquely identified and can be checked and audited

Recommendation

Compliant

LOCARD SELP Results Details

71

71

Assessment Number: SELP.V4.1.036

Assessment Description

Is there any other way that the LOCARD system will use methods, such as on-chain and off-chain storage of personal data, in order to reach as close as possible to the data erasure?

Response

Compliant

LOCARD uses the storage datasets for the evidence and other data, and blockchain only for hashes (minimal on-chain information). Data are connected by unique IDs. This approach guarantees the use of the proper deletion mechanisms and prevents the issue of storing personal data on-chain.

Recommendation

Compliant

LOCARD SELP Results Details

72

72

Assessment Number: SELP.V4.1.037

Assessment Description

In a case where a court orders to transfer a piece of evidence (containing personal data) from the LOCARD system to other system(s) where **no Blockchain like platform is available**, what would be the mechanisms then? Please also comment here on the technicality involved and the time taken by the LOCARD system.

Response

Compliant

The mechanism will be precisely the same channels currently used by LEAs or end-users to send evidence. This protocols are tied to each jurisdiction and out of scope of LOCARD. LOCARD enables the flow of transferring an evidence, thus the evidence will appear as transferred in the system if required for the investigation purposes despite the other end point not having a LOCARD system. Further materials can be manually uploaded to complement the investigation and guarantee the full chain of custody, such as uploading manually e.g. a signed file related to the proper transfer of the case or an evidence to another end user.

Recommendation

Compliant

LOCARD SELP Results Details

73

73

Assessment Number: SELP.V4.1.038

Assessment Description

In a case where a court orders to transfer a piece of evidence (containing personal data) from the LOCARD system to other system(s) where **a Blockchain like platform is available**, what would be mechanisms then? Please also comment here on the technicality involved and the time taken by the LOCARD system.

Response

Compliant

The mechanism will be precisely the same channels currently used by LEAs or end-users to send a case and the related material if needed. This protocols are tied to each jurisdiction and out of scope of LOCARD. LOCARD enables the flow of transferring a case, thus the data related to a case will appear as transferred in the system if required for the investigation purposes despite the other end point not having a LOCARD system. Further materials can be manually uploaded to complement the investigation and guarantee the full chain of custody, such as uploading manually e.g. a signed file related to the proper transfer of the case or an evidence to another end user.

Recommendation

Compliant

LOCARD SELP Results Details

74

74

Assessment Number: SELP.V4.1.039

Assessment Description

Can the investigator/authority, using the LOCARD system, provide the data subject the information relating to him/her in a concise, transparent, intelligible, and easily accessible form by using clear and plain language? How much time can the system need to perform this task?.

Response

Compliant

This is in the crowdsource intelligence engine. All the info related to a user rights and etc is shown there almost immediately.

Recommendation

Compliant.

LOCARD SELP Results Details

75

75

Assessment Number: SELP.V4.1.040

Assessment Description

What level of robustness and system security does the LOCARD platform guarantee against in and 0-order vulnerabilities?

Response

Compliant

The work being done is described in deliverable D6.5, (Summary of the security analysis made by Neurosoft). This document provides a profound understanding of the security built into LOCARD.

Recommendation

Compliant.

LOCARD SELP Results Details

76

76

LOCARD SELP Conclusions

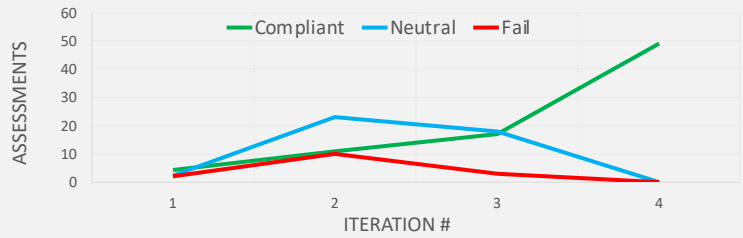
77

77

Conclusions

Based on the current development of the LOCARD system and the analysis of the responses gathered from the concerned partners on the SELP requirements previously marked as 'neutral' and 'fail', the LOCARD platform meets all Social, Ethical, Legal and Privacy requirements set out in the SELP Benchmark Report deliverable D2.1 and previous recommendations. Now, the platform/architecture has reached the 'pass' status against all the SELP requirements set in the beginning to test the LOCARD system/tools throughout its lifetime. On top of this, the system has achieved the necessary number of requirements on the MoScoW labelling. The platform is fully capable of providing adequate protection to the rights and freedoms of individuals.

Project Progress



Overall Project Performance

LOCARD SELP Results Summary

78

78

Conclusions

In iteration 3, requirements regarding the physical location and security of email chats were put under the 'fail' category. However, the LOCARD current development negates this previous assessment. The system provides flexibility to the organization to provide similar protection to the email chats if they hold evidentiary value. If the chats are of general purposes and are part of the communication between authorities, there is no need to log them as evidence. Apart from this specific case, requirements that were assessed previously as 'neutral' such as actions related to the mirrored websites, information required for the LOCARD user registration, the physical location of evidence storage, overviewing of the applicability and compliance of smart contracts, etc., have met the respective recommendations. As a recommendation for the end-users, the LOCARD platform provides some degree of flexibility in terms of data storage on the local databases or in the cloud. It will depend on the organisation to protect personal data stored on the cloud in accordance with the EU and applicable national laws. A local administrator should manage access to the LOCARD platform, and the concerned organization must incorporate policies regarding criminal liability for the users in a case when a false accusation is made by the platform user itself or when the user allows such accusations to the system knowingly. A clarification on this account should be provided in the user manual.

79

79

LOCARD

May 2022

https://locard.eu/contact

80

80