



Intelligence Network & Secure Platform for Evidence Correlation and Transfer

D8.6: Ethical, Legal and Social requirements for the INSPECTr platform and tools

Document Summary Information

Grant Agreement No	833276	Acronym	INSPECTr
Full Title	Intelligence Network & Secure Platform for Evidence Correlation and Transfer		
Start Date	01/09/2019	Duration	42 months
Project URL	https://www.inspectr-project.eu		
Deliverable	D8.6: Ethical, Legal and Social requirements for the INSPECTr platform and tools		
Work Package	WP 8		
Contractual due date	28.02.23	Actual submission date	06.03.23
Nature	R	Dissemination Level	PU
Lead Beneficiary	TRI		
Responsible Author	Dr Joshua Hughes		
Contributions from	Dr David Barnard-Wills, David Wright		

Revision history (including peer reviewing & quality control)

Version	Issue Date	% Complete	Changes	Contributor(s)
V0.1	01.12.22		Initial structure	Joshua Hughes
V0.2	24.01.23		Initial drafting	Joshua Hughes, David Wright, David-Barnard Wills
V0.3	14.02.23		Peer Review	Jeanne Mifsud Bonnici
V0.4	27.02.23		EAB Review	Daragh O'Brien
v1.0	03.03.23	100	Final edits	Joshua Hughes

Disclaimer

The content of the publication herein is the sole responsibility of the publishers and it does not necessarily represent the views expressed by the European Commission or its services.

While the information contained in the documents is believed to be accurate, the authors(s) or any other participant in the INSPECTr consortium make no warranty of any kind with regard to this material including, but not limited to the implied warranties of merchantability and fitness for a particular purpose.

Neither the INSPECTr Consortium nor any of its members, their officers, employees or agents shall be responsible or liable in negligence or otherwise howsoever in respect of any inaccuracy or omission herein.

Without derogating from the generality of the foregoing neither the INSPECTr Consortium nor any of its members, their officers, employees or agents shall be liable for any direct or indirect or consequential loss or damage caused by or arising from any information advice or inaccuracy or omission herein.

Copyright message

© INSPECTr Consortium, 2019-2023. This deliverable contains original unpublished work except where clearly indicated otherwise. Acknowledgement of previously published material and of the work of others has been made through appropriate citation, quotation or both. Reproduction is authorised provided the source is acknowledged.

Table of Contents

1	Introduction.....	5
1.1	Mapping INSPECTr Outputs	5
1.2	Deliverable Overview and Report Structure	7
2	Methodology	8
3	INSPECTr Ethical, Legal and Social Requirements	9
4	Assessment of efforts to fulfil requirements.....	14
5	Horizon scanning and sensitization efforts	63
5.1	Post-project exploitation risks	63
5.2	Policy proposals regarding end-to-end encryption.....	64
5.3	Anonymisation of sensitive personal data.....	64
6	Conclusions.....	66

List of Tables

Table 1: Adherence to INSPECTr GA Deliverable & Tasks Descriptions5

Table 2: INSPECTr Ethics Requirements (January 2021)9

Glossary of terms and abbreviations used

Abbreviation / Term	Description
AI	Artificial intelligence
AI HLEG	High-Level Expert Group on Artificial Intelligence
CFR	Charter of Fundamental Rights of the European Union
DPIA	Data Protection Impact Assessment
EAB	Ethics Advisory Board
EC	European Commission
ECHR	European Convention of Human Rights (ECHR)
EDPS	European Data Protection Supervisor
EGE	European Group on Ethics in Science and New Technologies
ELSI	Ethical, legal and social issues
EU	European Union
GDPR	General Data Protection Regulation
Ibid.	<i>Ibidem</i> (reference is the same as the preceding one)
IEEE	Institute of Electrical and Electronic Engineers
LEA	Law Enforcement Authority
LED	Law Enforcement Directive
TFEU	Treaty on the Functioning of the European Union
TRI	Trilateral Research Ltd.
WP	Work Package

1 Introduction

This deliverable follows on from previous deliverable *D8.5: Ethical, Legal and Social requirements for the INSPECTr platform and tools* that outlined key ethical, legal, and societal concepts and applied them to the INSPECTr technologies in the form of requirements. This document reviews those concepts and assesses compliance with the relevant requirements for each INSPECTr technology.

The requirements discussed in this deliverable relate to the INSPECTr components as technologies with a view toward them being used by law enforcement agencies (LEAs). Requirements for the INSPECTr project *as a research project* are covered in WP9. It is important to note at the outset that, whilst the INSPECTr technologies have been researched and developed with the aim of eventual operational use by LEAs, the outcome of research projects are not generally amenable to being procured by LEAs straight after a project ends. There are often ‘last-mile’ developments that need to be completed before research outputs can be considered as ‘products’, or as completely ‘usable’ in the LEA context. As such, not all the INSPECTr technologies are ‘finished’ in this sense so the INSPECTr technologies do not meet all of the requirements outlined below, and nor should we always expect them to. As these technologies have been developed in a research project, we cannot expect the same levels of quality assurance and testing that takes place in industry. In any case, it is important that such technologies are researched and developed in ways that take account of ethical, legal, and societal considerations and this is what are applied to the INSPECTr technologies below. Indeed, most requirements have been met by most tools and so we can say that the development of the INSPECTr technologies have gone a substantial way toward these technologies being considered as ‘trustworthy’ or ‘responsible’ AI.

The requirements have been informed by the Ethics Governance processes and tools detailed in deliverable *D8.4: Third Report on Ethical Governance*, and also have influenced the ethics and privacy-by-design process outlined in *D8.7: Privacy and Ethics-by-design in the INSPECTr platform* and *D8.8: Guide on privacy and ethics-by-design in law enforcement technology*.

1.1 Mapping INSPECTr Outputs

The purpose of this section is to map INSPECTr Grant Agreement commitments, both within the formal Deliverable and Task description, against the project’s respective outputs and work performed.

Table 1: Adherence to INSPECTr GA Deliverable & Tasks Descriptions

INSPECTr GA Component Title	INSPECTr GA Component Outline	Respective Document Chapter(s)	Justification
DELIVERABLE			
<i>D8.6: Ethical, Legal and Social requirements for the INSPECTr platform and tools</i>	<i>Final Report, on Horizon scanning and Sensitisation of Consortium.</i>	<i>Sections 3 and 4</i>	<i>Section 3 assesses the compliance status for each INSPECTr technology . Section 4 explains horizon scanning and sensitisation efforts.</i>

TASKS			
<p><i>T8.2 Ethical, legal and social issues and requirements for the INSPECTr Platform and Tools.</i></p>	<p><i>ST8.2.1 Issues and requirements. This task will undertake a sociological examination of the main ethical, legal and social issues (ELSI) that are relevant to INSPECTr's technologies in their operational environments. Further ethical and societal aspects of gender will be reviewed ... The partners will consult with stakeholders to gather their views on the ELSI that might arise from within INSPECTr. The results will be a set of privacy and ethical requirements ...</i></p> <p><i>ST8.2.2 Horizon scanning. (m12-m36) scanning the horizon for ethical issues that could arise in relation to digital forensics, by reviewing items in ethics and technology journals, social media, articles in the professional press, the proceedings of digital forensics and technology ethics conferences, the news media, and other sources.</i></p> <p><i>ST8.2.3 Sensitisation of the consortium. [TRI]. Sensitisation of the consortium to interdisciplinary privacy, ethical and societal issues through initial workshops and regular conference calls. It will provide an overview of these issues for the benefit of the living labs and technology developers.</i></p> <p><i>....</i></p>	<p><i>Sections 3 and 4</i></p>	<p><i>Section 3 evaluates each INSPECTr technology against the ethical, legal, and societal issues previously outlined in the INSPECTr project.</i></p> <p><i>Section 4 explains efforts at horizon scanning and sensitisation of the INSPECTr consortium.</i></p>

1.2 Deliverable Overview and Report Structure

Section 2 briefly outlines the methodology used for implementing and assessing compliance with the ethical, legal, and societal requirements previously developed in *D8.5: Ethical, Legal and Social requirements for the INSPECTr platform and tools*

Section 3 sets out the relevant requirements and analyses the compliance of each INSPECTr technology with those requirements.

Section 4 provides information on key topics examined and discussed as part of horizon scanning and sensitisation efforts in the second half of the INSPECTr project.

2 Methodology

The previous deliverable *D8.5: Ethical, Legal and Social requirements for the INSPECTr platform and tools* examined frameworks used for analysing ethical, legal, and societal issues in research projects like INSPECTr. It went on to apply these frameworks to the INSPECTr technologies specifically and developed 22 requirements to be fulfilled by the INSPECTr technical development team; three additional requirements were added as the project progressed.

Trilateral have been available to technical partners throughout the project to discuss the requirements and how they can be implemented. Fulfilment of the recommendations was monitored via a spreadsheet that was shared with technical partners who were asked to explain how the components they were developing met the requirements. Taking these responses from technical partners, this deliverable assesses how the components meet these requirements.

This deliverable also explains continuing efforts regarding horizon scanning and explains the work done to sensitise the consortium to the issues, and how the project responded to emerging issues.

3 INSPECTr Ethical, Legal and Social Requirements

The below requirements were originally outlined in *D8.5: Ethical, Legal and Social requirements for the INSPECTr platform and tools*. They were updated when that deliverable was revised and some general information on implementation across the INSPECTr technologies was included.

Table 2: INSPECTr Ethics Requirements (from January 2021)

#	Requirement Specification	Measurement
1	Platform and Tools: Consider an initial pop-out whereby LEA agrees to lawful basis for use.	Pop-out(s) requiring confirmation of legal basis before the investigator can use an INSPECTr tool exists.
	Having an end-user agree to lawful use of the tools every time they use them could become cumbersome and ineffective. LEAs would need to agree to lawful use of the tools upon receipt of them. Specific operational use would be at the discretion of the LEAs themselves.	
2	Rules engine should be accompanied by clear guidance on its limitations, concerning the varied nature of legal systems, the evolving nature of law, including case law.	Information on rules engine limitations embedded into technology.
	This will be covered in training materials.	
3	All INSPECTr analysers are disabled by default and are individually enabled by LEA senior personnel.	Analysers disabled on first LEA use.
	This is expected to happen, with individual tools enabled by individual LEAs.	
4	Each INSPECTr analyser to be accompanied by detailed information on its functionality allowing senior LEA personnel to decide on the appropriateness of each release.	Clear information pack setting out individual analysers, their benefits and risks to accompany Platform and Tool.
	This will be incorporated into the training materials, and there will be a description of each tool provided in cortex within each docker.	
5	All INSPECTr web-based analysers to be accompanied by a traffic light protocol to identify the security level for the data accessed, e.g., TLP:AMBER.	Analysers that access the web include security level classification via 'Traffic Light Protocol'.
	As noted above, a TLP is planned to be implemented across the platform rather than just for web analysers	
6	Web Scraper Tool to encrypt collected data. <ul style="list-style-type: none"> Developers and LEAs to consider which investigators and how investigators decrypt 	Web scraper data automatically encrypted.

	data with a view to ensuring data minimisation.	
	Decisions on how data should be treated are expected to be made by the end-user. As such, data is unlikely to be encrypted automatically. However, data segregation would mean that the officer actually engaging in scraping would be the only person able to view that data unless they choose to specifically share it with another.	
7	<p>Web Scraper Tool include filter functionality to provide for limited data gathering where appropriate.</p> <ul style="list-style-type: none"> Web scraper design team to consult LEAs on common judicial preferences on filtering to reflect the legal concept of proportionality and to reflect this in so far as is possible in the technical composition. 	Web scraper includes personal data filtering functions.
	Filters could be implemented to limit data collection where needed.	
8	Web Scraper Tool design team to consider how the project can avoid unintentional gathering of personal data using filters when the data is located at unusual positions/points on webpage.	Additional web scraper personal data filtering function to be added to capture this requirement.
	Filters are available to prevent excessive data collection.	
9	Computer Vision Tool functionality to be limited to data stored on the INSPECTr Platform.	Computer Vision Tools only compatible with data stored on INSPECTr as LEA evidence.
	The computer vision tools can only be used with data inside of the INSPECTr platform. There is no plan to facilitate INSPECTr access to live data (e.g., real-time CCTV images).	
10	Suspect and Criminal Profiling Tool to be limited to data stored on the INSPECTr Platform.	Suspect and Criminal Profiling Tool only compatible with data stored on INSPECTr as LEA evidence.
	As above.	
11	LEAs should be able to delete their data across the INSPECTr Platform and Tools with relative ease. This means that developers should ensure that data residue is avoided on the Platform and in Tools.	LEA able to delete their INSPECTr data across the Platform in a limited number of steps.

	This function is still in development as the details of the Storage Element Service (SES) and Case Management System are not yet finalised. However, almost all data can be cleaned by the SES, with part-filled (i.e., failed) attempts to write data cleaned during the writing process. Metadata is stored on blockchain and kept in log files.	
12	<p>The design team in consultation with LEAs should consider the automated deletion of data, with prompts alerting LEAs to proactively continue storage.</p> <ul style="list-style-type: none"> This is advised especially for INSPECTr network data that has been obscured, such as ‘queries’ between Member State LEAs. 	Automated deletion time frames established, requiring investigator to proactively choose continued storage.
	All data that can be deleted manually can also be deleted automatically via a ‘cron-job’ (i.e., a chronologically timed action). Data could be flagged for keeping longer and not be subject to a cron-job; for example, an alert could be made a week before a cron-job is due to activate.	
13	All AI systems must seek to adjust existing models for bias to the full extent feasible, e.g., available adjustment data.	Design team to communicate known bias in datasets to LEAs and to identify adjustments made.
	Generally, the models to be provided to LEAs will include information on biases with adjustment measures taken depending on the biases. Where possible, newer models will be provided, and for some tools LEAs will be able to re-train them if biases are found (e.g. the Toolbox: Cross-correlation tool). Other bias mitigation work that requires a proof of concept work could be included in T4.5.4.	
14	<p>All AI systems must display possible bias or reporting issues, according to relative weights in the model, alongside the results of analysis.</p> <ul style="list-style-type: none"> Design teams to consider Bayesian or other related approaches for dealing with bias. 	Only AI models that account for uncertainty in data used by design team.
	Confidence levels will be reports, and information on residual biases will be discussed in the tool documentation and will be covered in the training materials.	
15	Selection of technical solutions, or decisions about technical features, must take into account how bias may emerge during operational use and the real-world impacts that might arise from this.	INSPECTr partners document possible real-world implications across all AI tools.
	LEA IT staff and operational officers would need to know about biases prior to installing and using the tools. As noted above, documentation and training materials will provide information on biases and how they could impact on LEA use of the tools.	
16	Representation of minority and marginalised groups is an evaluation criterion for participation in testing and capacity building workshops. This includes, but is not limited to: sex; gender; ethnicity; socio-economic background; disability, and; physical appearance.	For otherwise equal candidates, persons from minority or marginalised groups should be preferred in the selection of participants in workshops and webinars.

	Where LEAs and stakeholders are invited to workshops and events, INSPECTr partners will make specific efforts to recruit marginalised persons. For example, asking LEAs to specifically distribute event invitations to, for example, women's or LGBT groups in their organisations.	
17	All AI systems (including systems labelling events and objects) must provide information on errors (e.g., false positives, false negatives) and other weaknesses (e.g., poorer performance on particular groups) in the model outputs to inform LEA decision making.	AI outputs accompanied by clear explanations on their limitations.
	Relevant information will be provided in manuals and training materials.	
18	All AI systems should provide direction to LEA investigators on how the output should be expressed in future case communications. <ul style="list-style-type: none"> Design teams to consider the weight of evidence approach, e.g., weak, inconclusive, strong etc. 	AI outputs accompanied by directions on how to communicate results in case file and to other criminal justice professionals.
	Tools will provide confidences as results, rather than a definitive answers or decisions. This is because evidence will likely be transferred into the INSPECTr platform without provenance, and so it would be difficult for the tools to be able to dictate how results should be expressed.	
19	Design teams to consider feasibility of 'masking' certain features in AI system outputs to assist LEAs with understanding the impact of different factors/features in the AI output.	AI outputs based on composite information to provide LEAs the capacity to remove individual factors so as to observe impact.
	Partners who are building tools from scratch (e.g., the Toolbox: natural language processing, and the Toolbox: image processing), there should be a function to allow comparison between documents that have been processed by the tool and the original documents. With other tools (e.g., the Toolbox: Cross-correlation, and Toolbox: Crime prediction), information on how the different AI features work will be provided in the documentation. For tools that are not built from scratch, it would not be possible to switch off layers in a neural network, for example, and nor would retraining be expected to provide a sufficient level of control, therefore information could also be provided in the documentation.	
20	Design teams to consider whether AI system outputs can be communicated to LEAs through a harmonised approach, without affecting accuracy of information communicated.	Various AI outputs communicated in harmonised way (to extent possible).
	At this stage, provision of results separately is favoured. However, this will be evaluated after demonstrations have been provided.	
21	In addition to explainable AI outputs, the INSPECTr Platform and Tools to include embedded 'Help' section providing fuller explanations to LEAs aimed towards	Synthesised INSPECTr training materials to be embedded in 'Help' sections of INSPECTr Platform.

	facilitating understanding outside of any training requirements.	
	This information could be provided in the training materials, with links to the training materials provided in the platform itself.	
22	A harmonised (project, as opposed to partner based) human evaluation process to be considered for all AI systems within design development. <ul style="list-style-type: none"> The human evaluation process to consider performance and understandability. 	INSPECTr partner identified to lead evaluation process across all AI tools.
	It is expected that results should be provided with the data that caused them so the results can be better understood by the end-users, and thereby generate trust in the quality of the model after several months of use.	

In D8.7 Privacy and Ethics-by-Design in the INSPECTr Platform, three additional requirements were added. These are discussed below.

#	Requirement Specification	Measurement
23	If they are more understandable, tools could present results confidences rather than a definitive answer to provide a more accurate picture to end-users.	N/A
	As with requirement 18, tools will provide confidences rather than a definitive answer.	
24	Training materials need to give end-users an adequate understanding of the tools, and so it is essential that it is communicated and understood what the tools can do, what the tools are intended for, and what the tools cannot do.	N/A
	This will be incorporated into training materials guidance on training material content, including these requirements has been provided to technical partners.	
25	Project tools must facilitate categorisation of categories of data-subject (e.g., suspect, criminal, victim, witness, etc.).	N/A
	Tags and descriptions related to evidence in the Case Management System (The Hive) can be updated to include these categories.	

4 Assessment of efforts to fulfil requirements

Having outlined the requirements, this document now moves to assess compliance with the requirements. During implementation, partners realized that some requirements were best dealt with using a platform-wide approach and so 'cross-platform' solutions are provided in the first table, before assessing each INSPECTr technology individually. However, as some requirements are specific to individual tools, those requirements that are not relevant to the tool being assessed are not included in the tables below.

Component Number	Component's Name	Component's Acronym	Related Task	Description	Owner
0	INSPECTr Platform	n/a	All	The INSPECTr platform (assessment covers cross-platform solutions)	INSPECTr technical partners

ELS REQUIREMENTS vs INSPECTr COMPONENTS			Details of fulfilment	Requirement completed? (yes/no)
No	ELS Requirement's description	Measurement - Verification Action		
1	Platform and Tools: Consider an initial pop-out whereby LEA agrees to lawful basis for use.	Pop-out(s) requiring confirmation of legal basis before the investigator can use an INSPECTr tool exists.	LEAs will agree to only use INSPECTr tools lawfully at the point of providing the INSPECTr tools. However, specific operational uses of the tools would be regulated at the level of individual LEAs; a reminder could be implemented at the log-in page to the case management system before use of any INSPECTr technologies.	Yes
2	Rules engine should be accompanied by clear guidance on its limitations, concerning the varied nature of legal systems, the evolving nature of law, including case law.	Information on rules engine limitations embedded into technology.	N/A - is relevant to all tools, and this will be resolved with the training courses and manuals	(Yes, guidance provided in training materials)

3	All INSPECTr analysers are disabled by default and are individually enabled by LEA senior personnel.	Analysers disabled on first LEA use.	Yes, INSPECTr analysers will be disabled by default. Individual LEA policies would decide on what tools can be used by their officers, and they will be enabled/disabled by administrators at LEAs via cortex.	Yes
4	Each INSPECTr analyser to be accompanied by detailed information on its functionality allowing senior LEA personnel to decide on the appropriateness of each release.	Clear information pack setting out individual analysers, their benefits and risks to accompany Platform and Tool.	Yes, detailed information on the functionality of each INSPECTr technology will be incorporated into the training materials. These will be available to senior LEA officers so that they can determine if the INSPECTr technologies are appropriate for their organisation. This information will also be included in Cortex to provide a description for the tools in each docker so that administrators and operational officers are aware of the functionality of each technology.	Yes
5	All INSPECTr web-based analysers to be accompanied by a traffic light protocol to identify the security level for the data accessed, e.g., TLP:AMBER.	Analysers that access the web include security level classification via 'Traffic Light Protocol'.	<p>A Traffic Light Protocol has been implemented for each INSPECTr tool to restrict the sharing and re-sharing of sensitive data. This assigns a rating of red, amber, green, or white (most sensitive to no sensitivity) to a particular dataset. For example, where information is captured by a web scraper, it might be possible to share moderately sensitive data (amber) across jurisdiction, but highly sensitive data (red) might need to remain with the LEA collecting the data.</p> <p>The INSPECTr maximum permissible actions protocol (MAX PAP) can also prevent particular actions taking place</p>	Yes

			<p>automatically on especially sensitive documents. If an LEA were to gather information about a criminal organisation operating online, they would probably not want such information being analysed automatically by tools beyond their direct control in case of data leaks. For example, automatically searching public databases for information on malware might alert a criminal organisation who are monitoring the database to the investigation; so such activities should be avoided for highly sensitive data. A high MAX PAP level would restrict any information being shared beyond the investigative team automatically, thereby minimising such risks.</p> <p>See also Section 2.1.2. of <i>D8.8: Guide on privacy and ethics-by-design in law enforcement technology</i> for more details on other capabilities for restricting data and technology access to qualified persons.</p>	
9	Computer Vision Tool functionality to be limited to data stored on the INSPECTr Platform.	Computer Vision Tools only compatible with data stored on INSPECTr as LEA evidence.	INSPECTr would only be used on stored data, not live data (e.g. real-time CCTV). All processing would be logged in INSPECTr on the blockchain.	Yes

10	Suspect and Criminal Profiling Tool to be limited to data stored on the INSPECTr Platform.	Suspect and Criminal Profiling Tool only compatible with data stored on INSPECTr as LEA evidence.	INSPECTr would only be used on stored data, not live data (e.g. real-time crime data feeds). All processing would be logged in INSPECTr on the blockchain.	Yes
11	LEAs should be able to delete their data across the INSPECTr Platform and Tools with relative ease. This means that developers should ensure that data residue is avoided on the Platform and in Tools.	LEA able to delete their INSPECTr data across the Platform in a limited number of steps.	Due to the complexity of the INSPECTr platform, it is not possible to wipe all data with relative ease (or at least to develop this within the project timeline). This is dealt with in more detail in relation to the SEs and CMS below. However, implementing a 'Blockhasher' could provide a pseudo-"wipe all" function	No
12	The design team in consultation with LEAs should consider the automated deletion of data, with prompts alerting LEAs to proactively continue storage. · This is advised especially for INSPECTr network data that has been obscured, such as 'queries' between Member State LEAs.	Automated deletion time frames established, requiring investigator to proactively choose continued storage.	Alerts to end-users could be implemented so that end-users are made aware of impending data deletion a week before data deletion. More details provided for SES.	No
13	All AI systems must seek to adjust existing models for bias to the full extent feasible, e.g., available adjustment data.	Design team to communicate known bias in datasets to LEAs and to identify adjustments made.	In ST4.5.4, GN considered the implications of adjusting models for bias, and spoke with other LEAs on the desirability of doing this. The result of this consideration and consultation was that LEAs were not in favour of adjusting models to reduce biases as this could impact on the evaluation of evidence which might create incorrect	No, but an alternative has been implemented.

			assumptions within an investigation. Further, GN made clear that as the models are highly complex, adjustments to models could have unforeseen consequences that might not actually create the less biased result desired. The project's Ethics Manager considered that although it would be advantageous from an ethical perspective to adjust models to minimise bias, the position of LEAs was understandable and the complexity of the models presented a risk of not being able to resolve bias. Therefore, rather than adjusting models on behalf of end users, the documentation for INSPECTr technologies should include information on bias risks and how end-users can recognise and mitigate these effects.	
14	All AI systems must display possible bias or reporting issues, according to relative weights in the model, alongside the results of analysis. · Design teams to consider Bayesian or other related approaches for dealing with bias.	Only AI models that account for uncertainty in data used by design team.	Confidence levels will be reported. Linked with the response to requirement 13, bias will be discussed in the documentation, and will be covered in the training and manuals.	
15	Selection of technical solutions, or decisions about technical features, must take into account how bias may emerge during operational use and the real-world impacts that might arise from this.	INSPECTr partners document possible real-world implications across all AI tools.	Relevant information from training material will be provided to senior LEA officers at the procurement stage. Administrators and operational officers would need to know about biases when installing the tools and using them so	Yes

			that the results are interpreted correctly.	
16	Representation of minority and marginalised groups is an evaluation criterion for participation in testing and capacity building workshops. This includes, but is not limited to: sex; gender; ethnicity; socio-economic background; disability, and; physical appearance.	For otherwise equal candidates, persons from minority or marginalised groups should be preferred in the selection of participants in workshops and webinars.	LEAs engaged in testing of INSPECTr tools have been asked to provide representative groups for testing. LEA officers engaged in testing are as representative as possible from the limited pool of persons engaged in the INSPECTr project.	Yes
17	All AI systems (including systems labelling events and objects) must provide information on errors (e.g., false positives, false negatives) and other weaknesses (e.g., poorer performance on particular groups) in the model outputs to inform LEA decision making.	AI outputs accompanied by clear explanations on their limitations.	Covered in manuals and training	Yes
18	All AI systems should provide direction to LEA investigators on how the output should be expressed in future case communications. · Design teams to consider the weight of evidence approach, e.g., weak, inconclusive, strong etc.	AI outputs accompanied by directions on how to communicate results in case file and to other criminal justice professionals.	Tools should provide confidences as results, rather than a definitive answer so that evidence can be understood more accurately.	Yes

19	Design teams to consider feasibility of 'masking' certain features in AI system outputs to assist LEAs with understanding the impact of different factors/features in the AI output.	AI outputs based on composite information to provide LEAs the capacity to remove individual factors so as to observe impact.	With tools that are not built from scratch (as some INSPECTr tools build on existing models/technologies), it would not be possible to switch off different layers. Retraining would not likely provide the same level of control. Switching off layers would likely have an impact on cross-case correlation, image recognition, and NLP tools. As such, a technical solution does not seem ideal. Instead, training manuals cover information on how LEA officers should interpret the results of the technological analysis.	Yes, this has been considered
20	Design teams to consider whether AI system outputs can be communicated to LEAs through a harmonised approach, without affecting accuracy of information communicated.	Various AI outputs communicated in harmonised way (to extent possible).	Due to the various data types being analysed, and the large number of technologies involved (not all of which will be used simultaneously), a unified approach has not been possible. Instead, the platform will provide separate results, especially where tools do the same thing (e.g., image recognition) so that end-users can understand the outputs in context and retain as much human agency as possible.	Yes, this has been considered
21	In addition to explainable AI outputs, the INSPECTr Platform and Tools to include embedded 'Help' section providing fuller explanations to LEAs aimed towards facilitating understanding outside of any training requirements.	Synthesised INSPECTr training materials to be embedded in 'Help' sections of INSPECTr Platform.	Will be covered in training materials. Links to training materials could be provided in platform.	Yes

22	<p>A harmonised (project, as opposed to partner based) human evaluation process to be considered for all AI systems within design development.</p> <ul style="list-style-type: none"> The human evaluation process to consider performance and understandability. 	INSPECTr partner identified to lead evaluation process across all AI tools.	Results should be provided with data that caused them so that it can be understood by the end-users, and then generate trust in the quality of the model after several months of use	Yes
23*	If they are more understandable, tools could present results confidences rather than a definitive answer to provide a more accurate picture to end-users.		Where possible, results will be provided with confidence levels	Yes
24*	Training materials need to give end-users an adequate understanding of the tools, and so it is essential that it is communicated and understood what the tools can do, what the tools are intended for, and what the tools cannot do.		This information is covered in training materials	Yes
25*	Project tools must facilitate categorisation of categories of data-subject (e.g., suspect, criminal, victim, witness, etc.).		Tags/description related to evidence in Hive can be updated to match these categories.	Yes

Component Number	Component's Name	Component's Acronym	Related Task	Description	Owner
1	PUB/SUB	PS	T3.1	The Federated end of the Publish-Subscribe Engine.	ILS

ELS REQUIREMENTS vs INSPECTr COMPONENTS			Details of fulfilment	Requirement completed? (yes/no)
No	ELS Requirement's description	Measurement - Verification Action		
2	Rules engine should be accompanied by clear guidance on its limitations, concerning the varied nature of legal systems, the evolving nature of law, including case law.	Information on rules engine limitations embedded into technology.	Guidance on the limitations of the technology will be included in the documentation material	Yes
11	LEAs should be able to delete their data across the INSPECTr Platform and Tools with relative ease. This means that developers should ensure that data residue is avoided on the Platform and in Tools.	LEA able to delete their INSPECTr data across the Platform in a limited number of steps.	Query History can be manually deleted via LabBox UI	Yes

12	The design team in consultation with LEAs should consider the automated deletion of data, with prompts alerting LEAs to proactively continue storage. · This is advised especially for INSPECTr network data that has been obscured, such as ‘queries’ between Member State LEAs.	Automated deletion time frames established, requiring investigator to proactively choose continued storage.	Query History is deleted regularly after a configurable retention period.	Yes
24*	Training materials need to give end-users an adequate understanding of the tools, and so it is essential that it is communicated and understood what the tools can do, what the tools are intended for, and what the tools cannot do.		Guidance on the limitations of the technology will be included in the documentation material	Yes

Component Number	Component's Name	Component's Acronym	Related Task	Description	Owner
2	Wrappers, API's, Parsers	WAP	T3.2.1-3	API's, parsers and wrappers to pull data from tools and into CASE format.	CCI

ELS REQUIREMENTS vs INSPECTr COMPONENTS			Details of fulfilment	Requirement completed? (yes/no)
No	ELS Requirement's description	Measurement - Verification Action		

2	Rules engine should be accompanied by clear guidance on its limitations, concerning the varied nature of legal systems, the evolving nature of law, including case law.	Information on rules engine limitations embedded into technology.	Guidance on the limitations of the technology will be included in the documentation material	Yes
24*	Training materials need to give end-users an adequate understanding of the tools, and so it is essential that it is communicated and understood what the tools can do, what the tools are intended for, and what the tools cannot do.		Guidance on the limitations of the technology will be included in the documentation material	Yes

Component Number	Component's Name	Component's Acronym	Related Task	Description	Owner
3	Dark Web Scraper	DWS	T3.2.4(a)	The federated dark web scraper that trawls for general data collection & indexing.	GN

ELS REQUIREMENTS vs INSPECTr COMPONENTS			Details of fulfilment	Requirement completed? (yes/no)
No	ELS Requirement's description	Measurement - Verification Action		

2	Rules engine should be accompanied by clear guidance on its limitations, concerning the varied nature of legal systems, the evolving nature of law, including case law.	Information on rules engine limitations embedded into technology.	Guidance on the limitations of the technology will be included in the documentation material	Yes
5	All INSPECTr web-based analysers to be accompanied by a traffic light protocol to identify the security level for the data accessed, e.g., TLP:AMBER.	Analysers that access the web include security level classification via 'Traffic Light Protocol'.	For now, the scrapper is a stand-alone tool that does not automatically connect to the TLP when data is collected. The user needs to determine the TLP level separately and then apply this to the collected data.	Yes
6	Web Scraper Tool to encrypt collected data. · Developers and LEAs to consider which investigators and how investigators decrypt data with a view to ensuring data minimisation.	Web scraper data automatically encrypted.	Not implemented at this stage, due to other priorities. However, data segregation should mean that any officer engaging in web scraping would be the only person able to view it. But encrypting data to facilitate sharing would need to be considered.	No
7	Web Scraper Tool include filter functionality to provide for limited data gathering where appropriate. · Web scraper design team to consult LEAs on common judicial preferences on filtering to reflect the legal concept of proportionality and to reflect this in so far as is possible in the technical composition.	Web scraper includes personal data filtering functions.	Filters were considered by GN and other LEAs. As suggested, this follows 'common judicial preferences'. However, as investigators need to be able to examine all available evidence, the use of filters would impair the investigative process.	No, but an alternative is implemented.

			Therefore, filters were not implemented as originally considered. Rather, to enable control over the total amount of personal data collected, the web scraper does not scrap all available data by default. For example, the scraper can be set to collect data from one web page only and not follow any links contained in it. Or, the tool can be set to follow certain links.	
8	Web Scraper Tool design team to consider how the project can avoid unintentional gathering of personal data using filters when the data is located at unusual positions/points on webpage.	Additional web scraper personal data filtering function to be added to capture this requirement.	As noted above, filters are not applied, but follow links is controlled.	Yes, this was considered and LEA partners decided against implementing filters as originally envisaged.
11	LEAs should be able to delete their data across the INSPECTr Platform and Tools with relative ease. This means that developers should ensure that data residue is avoided on the Platform and in Tools.	LEA able to delete their INSPECTr data across the Platform in a limited number of steps.	All the results of the scrapper are stored in one single file that can be deleted.	Yes

12	The design team in consultation with LEAs should consider the automated deletion of data, with prompts alerting LEAs to proactively continue storage. · This is advised especially for INSPECTr network data that has been obscured, such as ‘queries’ between Member State LEAs.	Automated deletion time frames established, requiring investigator to proactively choose continued storage.	Not implemented as different LEAs have different needs, which need to be understood before this can be implemented.	No
24*	Training materials need to give end-users an adequate understanding of the tools, and so it is essential that it is communicated and understood what the tools can do, what the tools are intended for, and what the tools cannot do.		Guidance on the limitations of the technology will be included in the documentation material	Yes
25*	Project tools must facilitate categorisation of categories of data-subject (e.g., suspect, criminal, victim, witness, etc.).		Not directly applicable. The scrapper collects all the information exactly as it is issued to guarantee traceability and that it can be used for forensic purposes. The data can then be categorised as needed during the next steps of an investigation.	Partially

Component Number	Component's Name	Component's Acronym	Related Task	Description	Owner
------------------	------------------	---------------------	--------------	-------------	-------

4	Toolbox: Block-hashing for Triage	tBH4T	T3.2.5	Block-hashing tool for categorising the content of digital storage devices	CCI
---	--	-------	---------------	--	-----

ELS REQUIREMENTS vs INSPECTr COMPONENTS			Details of fulfilment	Requirement completed? (yes/no)
No	ELS Requirement's description	Measurement - Verification Action		
2	Rules engine should be accompanied by clear guidance on its limitations, concerning the varied nature of legal systems, the evolving nature of law, including case law.	Information on rules engine limitations embedded into technology.	Guidance on the limitations of the technology will be included in the documentation material	Yes
11	LEAs should be able to delete their data across the INSPECTr Platform and Tools with relative ease. This means that developers should ensure that data residue is avoided on the Platform and in Tools.	LEA able to delete their INSPECTr data across the Platform in a limited number of steps.	The tool provides a mechanism to wipe the database, if it becomes compromised by inaccurate data.	Yes
23*	If they are more understandable, tools could present results confidences rather than a definitive answer to provide a more accurate picture to end-users.		Tool output will indicate if any category has been validated. In some cases ("QuickScan") the data is only an indication and this will be indicated to the user.	Yes

24*	Training materials need to give end-users an adequate understanding of the tools, and so it is essential that it is communicated and understood what the tools can do, what the tools are intended for, and what the tools cannot do.		Guidance on the limitations of the technology will be included in the documentation material	Yes
-----	---	--	--	-----

Component Number	Component's Name	Component's Acronym	Related Task	Description	Owner
5	Data Ingestion & Orchestration Engine	CORTEX	T3.3.1,3	The underlying system invokes the analytics and handles all the data flows.	SIREN

ELS REQUIREMENTS vs INSPECTr COMPONENTS			Details of fulfilment	Requirement completed? (yes/no)
No	ELS Requirement's description	Measurement - Verification Action		
2	Rules engine should be accompanied by clear guidance on its limitations, concerning the varied nature of legal systems, the evolving nature of law, including case law.	Information on rules engine limitations embedded into technology.	Guidance on the limitations of the technology will be included in the documentation material	Yes

19	Design teams to consider feasibility of 'masking' certain features in AI system outputs to assist LEAs with understanding the impact of different factors/features in the AI output.	AI outputs based on composite information to provide LEAs the capacity to remove individual factors so as to observe impact.	Data Masking options available in Elastic search configurable as needed.	Yes
24*	Training materials need to give end-users an adequate understanding of the tools, and so it is essential that it is communicated and understood what the tools can do, what the tools are intended for, and what the tools cannot do.		Guidance on the limitations of the technology will be included in the documentation material	Yes
25*	Project tools must facilitate categorisation of categories of data-subject (e.g., suspect, criminal, victim, witness, etc.).		Data can be categorised by subject using an Analyzer.	yes

Component Number	Component's Name	Component's Acronym	Related Task	Description	Owner
6	Storage Element Service	SES	T3.3.2	Storage layer w/ Neo4j, Mongo, Elastic Search – a	VLTN

				standalone w/ wrapper in CORTEX	
--	--	--	--	---------------------------------	--

ELS REQUIREMENTS vs INSPECTr COMPONENTS			Details of fulfilment	Requirement completed? (yes/no)
No	ELS Requirement's description	Measurement - Verification Action		
2	Rules engine should be accompanied by clear guidance on its limitations, concerning the varied nature of legal systems, the evolving nature of law, including case law.	Information on rules engine limitations embedded into technology.	Guidance on the limitations of the technology will be included in the documentation material	yes
11	LEAs should be able to delete their data across the INSPECTr Platform and Tools with relative ease. This means that developers should ensure that data residue is avoided on the Platform and in Tools.	LEA able to delete their INSPECTr data across the Platform in a limited number of steps.	Almost all data can be cleaned by the SES. Part-failed attempts to write data can be cleaned during the (failed) writing process by INSPECTr tools. Metadata is stored on the blockchain and kept in log files. From the point of the SES, deletion can take place via an API (where administrator-like access is necessary)	yes

12	The design team in consultation with LEAs should consider the automated deletion of data, with prompts alerting LEAs to proactively continue storage. · This is advised especially for INSPECTr network data that has been obscured, such as ‘queries’ between Member State LEAs.	Automated deletion time frames established, requiring investigator to proactively choose continued storage.	What can be deleted manually from the API, can also be deleted automatically via the same or different API using cron-jobs (i.e., actions that take place at a set time, or time sequence). Data could be flagged for keeping and not deleted by cron-jobs (via the CMS), by an end-users requesting extensions. For example, extending the time limit for data deletion.	Yes
24*	Training materials need to give end-users an adequate understanding of the tools, and so it is essential that it is communicated and understood what the tools can do, what the tools are intended for, and what the tools cannot do.		Guidance on the limitations of the technology will be included in the documentation material	yes

Component Number	Component's Name	Component's Acronym	Related Task	Description	Owner
7	Meta 2 Blockchain	M2B	T3.3.2	Module to Log all actions on HIVE and CORTEX to Blockchain	CCI

ELS REQUIREMENTS vs INSPECTr COMPONENTS	Details of fulfilment	Requirement completed?
--	------------------------------	-------------------------------

No	ELS Requirement's description	Measurement - Verification Action		(yes/no)
2	Rules engine should be accompanied by clear guidance on its limitations, concerning the varied nature of legal systems, the evolving nature of law, including case law.	Information on rules engine limitations embedded into technology.	Guidance on the limitations of the technology will be included in the documentation material	Yes
24*	Training materials need to give end-users an adequate understanding of the tools, and so it is essential that it is communicated and understood what the tools can do, what the tools are intended for, and what the tools cannot do.		Guidance on the limitations of the technology will be included in the documentation material	yes

Component Number	Component's Name	Component's Acronym	Related Task	Description	Owner
8	NLP for Legislation Management	LMN	T3.4.1.B	Natural Language Processing tools to extract relevant information	ILS

ELS REQUIREMENTS vs INSPECTr COMPONENTS			Details of fulfilment	Requirement completed? (yes/no)
No	ELS Requirement's description	Measurement - Verification Action		

2	Rules engine should be accompanied by clear guidance on its limitations, concerning the varied nature of legal systems, the evolving nature of law, including case law.	Information on rules engine limitations embedded into technology.	Component's output will only be used as consultation by LEAs. However, disclaimers and explanation within documentation will be included.	Yes
12	The design team in consultation with LEAs should consider the automated deletion of data, with prompts alerting LEAs to proactively continue storage. · This is advised especially for INSPECTr network data that has been obscured, such as 'queries' between Member State LEAs.	Automated deletion time frames established, requiring investigator to proactively choose continued storage.	Component only stores data temporarily in-container.	Yes
13	All AI systems must seek to adjust existing models for bias to the full extent feasible, e.g., available adjustment data.	Design team to communicate known bias in datasets to LEAs and to identify adjustments made.	Models offered will include information on any biases that are discussed in up-to-date bibliography. Measures will be taken according to what is suggested in the bibliography.	Yes. While total bias mitigation has not been possible, information on remaining biases are provided to the end-user to understand the implications of this.
14	All AI systems must display possible bias or reporting issues, according to relative weights in the model, alongside the results of analysis. · Design teams to consider Bayesian or other related approaches for dealing with bias.	Only AI models that account for uncertainty in data used by design team.	Results are provided with a level of confidence (%) where applicable.	Yes

15	Selection of technical solutions, or decisions about technical features, must take into account how bias may emerge during operational use and the real-world impacts that might arise from this.	INSPECTr partners document possible real-world implications across all AI tools.	D3.4 will explain how bias can arise according to own knowledge/testing and related bibliography. ¹	Yes
17	All AI systems (including systems labelling events and objects) must provide information on errors (e.g., false positives, false negatives) and other weaknesses (e.g., poorer performance on particular groups) in the model outputs to inform LEA decision making.	AI outputs accompanied by clear explanations on their limitations.	Documentation will discuss this. Output can also always include a disclaimer if required.	Yes
18	All AI systems should provide direction to LEA investigators on how the output should be expressed in future case communications. · Design teams to consider the weight of evidence approach, e.g., weak, inconclusive, strong etc.	AI outputs accompanied by directions on how to communicate results in case file and to other criminal justice professionals.	AI output will be used as consultation to LEAs on creating rules. It will not be written in CASE.	Yes

¹ D3.4 states: 'Before continuing, the reader and user of this tool should keep in mind that there are several limitations related to the usage of AI in real life situations. One limitation is the potential for bias in the data used to train the AI system, which can lead to biased or unfair outcomes in decision-making. Moreover, the lack of transparency in how AI systems make decisions, which can make it difficult for users to understand and trust the outcomes produced by the system. It follows, that it is important to continuously monitor and evaluate the performance of the model to ensure that it is producing fair and unbiased results. However, it should be noted that during development, we have not viewed any cases of bias while testing.'

20	Design teams to consider whether AI system outputs can be communicated to LEAs through a harmonised approach, without affecting accuracy of information communicated.	Various AI outputs communicated in harmonised way (to extent possible).	Documentation will discuss this. Output can also always include a disclaimer if required.	Yes
24*	Training materials need to give end-users an adequate understanding of the tools, and so it is essential that it is communicated and understood what the tools can do, what the tools are intended for, and what the tools cannot do.		Guidance on the limitations of the technology will be included in the documentation material	Yes

Component Number	Component's Name	Component's Acronym	Related Task	Description	Owner
9	Legal ACL Reasoning Engine	LAC	T3.4.1.C	Reasoning Engine to create a rule and provide an ACL for queries	EBOS

ELS REQUIREMENTS vs INSPECTr COMPONENTS			Details of fulfilment	Requirement completed? (yes/no)
No	ELS Requirement's description	Measurement - Verification Action		

2	Rules engine should be accompanied by clear guidance on its limitations, concerning the varied nature of legal systems, the evolving nature of law, including case law.	Information on rules engine limitations embedded into technology.	Rules will be set by LEAs from suggested parameters extracted by the legislation management tool from the database of legislation. Information on legal reasoning engine limitations can be provided in documentation while "varied nature of legal systems etc." is explained in depth in D2.1	Yes
24*	Training materials need to give end-users an adequate understanding of the tools, and so it is essential that it is communicated and understood what the tools can do, what the tools are intended for, and what the tools cannot do.		Guidance on the limitations of the technology will be included in the documentation material	Yes

Component Number	Component's Name	Component's Acronym	Related Task	Description	Owner
10	Information Request Management Engine	IRME	T3.4.2	Client-side of the PUBSUB Engine w/ Query generation and graph searching facilities	ILS

ELS REQUIREMENTS vs INSPECTr COMPONENTS	Details of fulfilment	Requirement completed?
---	-----------------------	------------------------

No	ELS Requirement's description	Measurement - Verification Action		(yes/no)
11	LEAs should be able to delete their data across the INSPECTr Platform and Tools with relative ease. This means that developers should ensure that data residue is avoided on the Platform and in Tools.	LEA able to delete their INSPECTr data across the Platform in a limited number of steps.	Data can be manually deleted via Portainer UI (1. stop IRME container-stack, 2. Delete docker volume, 3. Restart IRME container stack)	Yes
12	The design team in consultation with LEAs should consider the automated deletion of data, with prompts alerting LEAs to proactively continue storage. · This is advised especially for INSPECTr network data that has been obscured, such as ‘queries’ between Member State LEAs.	Automated deletion time frames established, requiring investigator to proactively choose continued storage.	Data are deleted regularly after a configurable retention period	Yes
24*	Training materials need to give end-users an adequate understanding of the tools, and so it is essential that it is communicated and understood what the tools can do, what the tools are intended for, and what the tools cannot do.		Guidance on the limitations of the technology will be included in the documentation material	yes

Component Number	Component's Name	Component's Acronym	Related Task	Description	Owner
------------------	------------------	---------------------	--------------	-------------	-------

11	INSPECTr Blockchain Ledger	IBL	T3.4.3	The blockchain ledger for INSPECTr	ILS
----	----------------------------	-----	---------------	------------------------------------	-----

ELS REQUIREMENTS vs INSPECTr COMPONENTS			Details of fulfilment	Requirement completed? (yes/no)
No	ELS Requirement's description	Measurement - Verification Action		
2	Rules engine should be accompanied by clear guidance on its limitations, concerning the varied nature of legal systems, the evolving nature of law, including case law.	Information on rules engine limitations embedded into technology.	The pop-up presented on the CMS at log-in could remind end-users that blockchain technology is used to store the logs in an immutable distributed ledger	Yes
11	LEAs should be able to delete their data across the INSPECTr Platform and Tools with relative ease. This means that developers should ensure that data residue is avoided on the Platform and in Tools.	LEA able to delete their INSPECTr data across the Platform in a limited number of steps.	Blockchain provides immutable storage of data, which means transactions cannot be removed. It is sufficient, and suitable for storage efficiently, to only store hashes of logs in order to satisfy this.	Yes
20	Design teams to consider whether AI system outputs can be communicated to LEAs through a harmonised approach, without affecting accuracy of information communicated.	Various AI outputs communicated in harmonised way (to extent possible).	Most probably alarms events will be pushed to the portal to be visualised	Yes

24*	Training materials need to give end-users an adequate understanding of the tools, and so it is essential that it is communicated and understood what the tools can do, what the tools are intended for, and what the tools cannot do.		Guidance on the limitations of the technology will be included in the documentation material	Yes
-----	---	--	--	-----

Component Number	Component's Name	Component's Acronym	Related Task	Description	Owner
12	Shared Knowledge Graph	SKG	T4.2(a)	The KG infrastructure to represent & link investigation data & observables from HIVE	VLTN

ELS REQUIREMENTS vs INSPECTr COMPONENTS			Details of fulfilment	Requirement completed? (yes/no)
No	ELS Requirement's description	Measurement - Verification Action		
11	LEAs should be able to delete their data across the INSPECTr Platform and Tools with relative ease. This means that developers should ensure that data residue is avoided on the Platform and in Tools.	LEA able to delete their INSPECTr data across the Platform in a limited number of steps.	Stores all data in SES, deletes everything else.	Yes

24*	Training materials need to give end-users an adequate understanding of the tools, and so it is essential that it is communicated and understood what the tools can do, what the tools are intended for, and what the tools cannot do.		Guidance on the limitations of the technology will be included in the documentation material	Yes
-----	---	--	--	-----

Component Number	Component's Name	Component's Acronym	Related Task	Description	Owner
13	Toolbox: Knowledge Graph	tKG	T4.2(b)	KG as a toolbox to represent subset data (e.g., dark web forum data) on a case by case	VLTN

ELS REQUIREMENTS vs INSPECTr COMPONENTS			Details of fulfilment	Requirement completed? (yes/no)
No	ELS Requirement's description	Measurement - Verification Action		
2	Rules engine should be accompanied by clear guidance on its limitations, concerning the varied nature of legal systems, the evolving nature of law, including case law.	Information on rules engine limitations embedded into technology.	Querying a knowledge graph for specific types of connections that would constitute an unlawful action could be prohibited, if they can be fully specified in nature. However, formalising human behaviour for machine-readable implementation is very difficult (especially	Yes

			where there are many exceptional circumstances in LEA investigations), and so this has not been pursued in the INSPECTr project.	
11	LEAs should be able to delete their data across the INSPECTr Platform and Tools with relative ease. This means that developers should ensure that data residue is avoided on the Platform and in Tools.	LEA able to delete their INSPECTr data across the Platform in a limited number of steps.	Stores all data in SES, deletes everything else.	Yes
24*	Training materials need to give end-users an adequate understanding of the tools, and so it is essential that it is communicated and understood what the tools can do, what the tools are intended for, and what the tools cannot do.		Guidance on the limitations of the technology will be included in the documentation material	yes

Component Number	Component's Name	Component's Acronym	Related Task	Description	Owner
14	Toolbox: Natural Language Processing	tNLP	T4.3.1	NLP toolbox to segment and classify discrete textual data e.g., SMS, WhatsApp, forum	ILS

ELS REQUIREMENTS vs INSPECTr COMPONENTS			Details of fulfilment	Requirement completed? (yes/no)
No	ELS Requirement's description	Measurement - Verification Action		
2	Rules engine should be accompanied by clear guidance on its limitations, concerning the varied nature of legal systems, the evolving nature of law, including case law.	Information on rules engine limitations embedded into technology.	Guidance on the limitations of the technology will be included in the documentation material	yes
11	LEAs should be able to delete their data across the INSPECTr Platform and Tools with relative ease. This means that developers should ensure that data residue is avoided on the Platform and in Tools.	LEA able to delete their INSPECTr data across the Platform in a limited number of steps.	Collects/stores all data from/in SES, deletes everything else.	Yes
13	All AI systems must seek to adjust existing models for bias to the full extent feasible, e.g., available adjustment data.	Design team to communicate known bias in datasets to LEAs and to identify adjustments made.	Models offered will include information on any biases that are discussed in up-to-date bibliography. Measures will be taken according to what is suggested in the bibliography.	Yes. While total bias mitigation has not been possible, information on remaining biases are provided to the end-user to understand the implications of this.

14	All AI systems must display possible bias or reporting issues, according to relative weights in the model, alongside the results of analysis. · Design teams to consider Bayesian or other related approaches for dealing with bias.	Only AI models that account for uncertainty in data used by design team.	Results will be provided with a level of confidence (%) where applicable (e.g., in sentiment analysis). For results that this is not applicable (e.g., NER), the relative success of during testing will be discussed in the documentation.	Yes
15	Selection of technical solutions, or decisions about technical features, must take into account how bias may emerge during operational use and the real-world impacts that might arise from this.	INSPECTr partners document possible real-world implications across all AI tools.	Documentation will mention/explain how bias can arise according to own knowledge/testing and related bibliography.	Yes
17	All AI systems (including systems labelling events and objects) must provide information on errors (e.g., false positives, false negatives) and other weaknesses (e.g., poorer performance on particular groups) in the model outputs to inform LEA decision making.	AI outputs accompanied by clear explanations on their limitations.	Documentation will discuss this. Output can also always include a disclaimer if required.	Yes
18	All AI systems should provide direction to LEA investigators on how the output should be expressed in future case communications. · Design teams to consider the weight of evidence approach, e.g., weak, inconclusive, strong etc.	AI outputs accompanied by directions on how to communicate results in case file and to other criminal justice professionals.	AI output is already in CASE.	Yes

19	Design teams to consider feasibility of 'masking' certain features in AI system outputs to assist LEAs with understanding the impact of different factors/features in the AI output.	AI outputs based on composite information to provide LEAs the capacity to remove individual factors so as to observe impact.	If analysed documents are edited by the LEAs, a comparison can be made between the edited and unedited documents.	Yes
20	Design teams to consider whether AI system outputs can be communicated to LEAs through a harmonised approach, without affecting accuracy of information communicated.	Various AI outputs communicated in harmonised way (to extent possible).	Documentation will discuss this. Output can also always include a disclaimer if required.	Yes
24*	Training materials need to give end-users an adequate understanding of the tools, and so it is essential that it is communicated and understood what the tools can do, what the tools are intended for, and what the tools cannot do.		Guidance on the limitations of the technology will be included in the documentation material	Yes

Component Number	Component's Name	Component's Acronym	Related Task	Description	Owner
------------------	------------------	---------------------	--------------	-------------	-------

15	Toolbox: Image Processing	tIP	T4.4.1	IP toolbox with models to segment and label image data inc. objects, CSAM etc.	CCI
----	----------------------------------	-----	---------------	--	-----

ELS REQUIREMENTS vs INSPECTr COMPONENTS			Details of fulfilment	Requirement completed? (yes/no)
No	ELS Requirement's description	Measurement - Verification Action		
2	Rules engine should be accompanied by clear guidance on its limitations, concerning the varied nature of legal systems, the evolving nature of law, including case law.	Information on rules engine limitations embedded into technology.	The pop-up could link to a documentation explaining the limitations. Visualisation should also contain a footnote with link to documentation	yes
9	Computer Vision Tool functionality to be limited to data stored on the INSPECTr Platform.	Computer Vision Tools only compatible with data stored on INSPECTr as LEA evidence.	Token authentication prevents access from outside the platform	Yes
11	LEAs should be able to delete their data across the INSPECTr Platform and Tools with relative ease. This means that developers should ensure that data residue is avoided on the Platform and in Tools.	LEA able to delete their INSPECTr data across the Platform in a limited number of steps.	No data is ever stored. Results are cached for 60 minutes.	Yes

13	All AI systems must seek to adjust existing models for bias to the full extent feasible, e.g., available adjustment data.	Design team to communicate known bias in datasets to LEAs and to identify adjustments made.	Dependent on dataset availability. Models can be swapped for newer versions.	Yes
14	All AI systems must display possible bias or reporting issues, according to relative weights in the model, alongside the results of analysis. · Design teams to consider Bayesian or other related approaches for dealing with bias.	Only AI models that account for uncertainty in data used by design team.	Results will be provided with a level of confidence (%) for all classes where applicable	yes
15	Selection of technical solutions, or decisions about technical features, must take into account how bias may emerge during operational use and the real-world impacts that might arise from this.	INSPECTr partners document possible real-world implications across all AI tools.	Documentation will mention/explain how bias can arise according to own knowledge/testing and related bibliography.	Yes
17	All AI systems (including systems labelling events and objects) must provide information on errors (e.g., false positives, false negatives) and other weaknesses (e.g., poorer performance on particular groups) in the model outputs to inform LEA decision making.	AI outputs accompanied by clear explanations on their limitations.	Documentation will discuss this. Output can also always include a disclaimer if required.	Yes

18	All AI systems should provide direction to LEA investigators on how the output should be expressed in future case communications. · Design teams to consider the weight of evidence approach, e.g., weak, inconclusive, strong etc.	AI outputs accompanied by directions on how to communicate results in case file and to other criminal justice professionals.	AI output is already in CASE.	Yes
19	Design teams to consider feasibility of 'masking' certain features in AI system outputs to assist LEAs with understanding the impact of different factors/features in the AI output.	AI outputs based on composite information to provide LEAs the capacity to remove individual factors so as to observe impact.	If analysed documents are edited by the LEAs, a comparison can be made between the edited and unedited documents.	yes
20	Design teams to consider whether AI system outputs can be communicated to LEAs through a harmonised approach, without affecting accuracy of information communicated.	Various AI outputs communicated in harmonised way (to extent possible).	Documentation will discuss this. Output can also always include a disclaimer if required.	Yes
24*	Training materials need to give end-users an adequate understanding of the tools, and so it is essential that it is communicated and understood what the tools can do, what the tools are intended for, and what the tools cannot do.		Guidance on the limitations of the technology will be included in the documentation material	Yes

25*	Project tools must facilitate categorisation of categories of data-subject (e.g., suspect, criminal, victim, witness, etc.).		Not applicable. tIP is subject agnostic	Partially, as compliance not possible but also does not impact on the subject of this requirement.
-----	--	--	---	--

Component Number	Component's Name	Component's Acronym	Related Task	Description	Owner
16	Toolbox: Capture Cracking	tCAP	T4.4.3	Computer vision tool to break Captcha found during webscraping	CCI

ELS REQUIREMENTS vs INSPECTr COMPONENTS			Details of fulfilment	Requirement completed? (yes/no)
No	ELS Requirement's description	Measurement - Verification Action		
2	Rules engine should be accompanied by clear guidance on its limitations, concerning the varied nature of legal systems, the evolving nature of law, including case law.	Information on rules engine limitations embedded into technology.	Guidance on the limitations of the technology will be included in the documentation material	Yes

24*	Training materials need to give end-users an adequate understanding of the tools, and so it is essential that it is communicated and understood what the tools can do, what the tools are intended for, and what the tools cannot do.		Guidance on the limitations of the technology will be included in the documentation material	Yes
-----	---	--	--	-----

Component Number	Component's Name	Component's Acronym	Related Task	Description	Owner
17	Toolbox: Cross-Correlation	tXC	T4.5.1	Toolbox to identify and extract similar data across different observables	GN

ELS REQUIREMENTS vs INSPECTr COMPONENTS			Details of fulfilment	Requirement completed? (yes/no)
No	ELS Requirement's description	Measurement - Verification Action		
2	Rules engine should be accompanied by clear guidance on its limitations, concerning the varied nature of legal systems, the evolving nature of law, including case law.	Information on rules engine limitations embedded into technology.	Guidance on the limitations of the technology will be included in the documentation material	Yes

10	Suspect and Criminal Profiling Tool to be limited to data stored on the INSPECTr Platform.	Suspect and Criminal Profiling Tool only compatible with data stored on INSPECTr as LEA evidence.	The tool is restricted to working on data on the INSPECTr platform only.	Yes
13	All AI systems must seek to adjust existing models for bias to the full extent feasible, e.g., available adjustment data.	Design team to communicate known bias in datasets to LEAs and to identify adjustments made.	Users can retrain/adjust some models on their own data	Yes, end-users can adjust models to mitigate resultant bias that are expected in their use-cases
17	All AI systems (including systems labelling events and objects) must provide information on errors (e.g., false positives, false negatives) and other weaknesses (e.g., poorer performance on particular groups) in the model outputs to inform LEA decision making.	AI outputs accompanied by clear explanations on their limitations.	Probabilities will be provided to the users rather than definitive answers. Weaknesses of the models will be disclosed in the documentation.	Yes
18	All AI systems should provide direction to LEA investigators on how the output should be expressed in future case communications. · Design teams to consider the weight of evidence approach, e.g., weak, inconclusive, strong etc.	AI outputs accompanied by directions on how to communicate results in case file and to other criminal justice professionals.	Covered by documentation material	Yes

19	Design teams to consider feasibility of 'masking' certain features in AI system outputs to assist LEAs with understanding the impact of different factors/features in the AI output.	AI outputs based on composite information to provide LEAs the capacity to remove individual factors so as to observe impact.	Covered by documentation material	Yes
20	Design teams to consider whether AI system outputs can be communicated to LEAs through a harmonised approach, without affecting accuracy of information communicated.	Various AI outputs communicated in harmonised way (to extent possible).	Documentation material	Yes
23*	If they are more understandable, tools could present results confidences rather than a definitive answer to provide a more accurate picture to end-users.		In most cases, probabilities are provided rather than definitive answers	Yes
24*	Training materials need to give end-users an adequate understanding of the tools, and so it is essential that it is communicated and understood what the tools can do, what the tools are intended for, and what the tools cannot do.		Guidance on the limitations of the technology will be included in the documentation material	Yes

25*	Project tools must facilitate categorisation of categories of data-subject (e.g., suspect, criminal, victim, witness, etc.).		We don't take into account the types, only the statistics of the categories	Partially, as compliance not possible but also does not impact on the subject of this requirement.
-----	--	--	---	--

Component Number	Component's Name	Component's Acronym	Related Task	Description	Owner
18	Toolbox: Network Analytics	tNA	T4.5.2	Toolbox for detection of existing links, analysing, detecting and profiling behaviours	SIREN

ELS REQUIREMENTS vs INSPECTr COMPONENTS			Details of fulfilment	Requirement completed? (yes/no)
No	ELS Requirement's description	Measurement - Verification Action		
2	Rules engine should be accompanied by clear guidance on its limitations, concerning the varied nature of legal systems, the evolving nature of law, including case law.	Information on rules engine limitations embedded into technology.	Guidance on the limitations of the technology will be included in the documentation material	Yes

19	Design teams to consider feasibility of 'masking' certain features in AI system outputs to assist LEAs with understanding the impact of different factors/features in the AI output.	AI outputs based on composite information to provide LEAs the capacity to remove individual factors so as to observe impact.	Data Masking options available in Elastic search configurable as needed.	Yes
24*	Training materials need to give end-users an adequate understanding of the tools, and so it is essential that it is communicated and understood what the tools can do, what the tools are intended for, and what the tools cannot do.		Guidance on the limitations of the technology will be included in the documentation material	yes
25*	Project tools must facilitate categorisation of categories of data-subject (e.g., suspect, criminal, victim, witness, etc.).		Data can be categorised by subject using an Analyzer.	yes

Component Number	Component's Name	Component's Acronym	Related Task	Description	Owner
19	Toolbox: Crime Prediction	tCP	T4.5.3	Examine relationship b/w historical crimes, and	GN

				geographic & temporal displacement	
--	--	--	--	------------------------------------	--

ELS REQUIREMENTS vs INSPECTr COMPONENTS			Details of fulfilment	Requirement completed? (yes/no)
No	ELS Requirement's description	Measurement - Verification Action		
2	Rules engine should be accompanied by clear guidance on its limitations, concerning the varied nature of legal systems, the evolving nature of law, including case law.	Information on rules engine limitations embedded into technology.	Guidance on the limitations of the technology will be included in the documentation material	yes
10	Suspect and Criminal Profiling Tool to be limited to data stored on the INSPECTr Platform.	Suspect and Criminal Profiling Tool only compatible with data stored on INSPECTr as LEA evidence.	The tool is restricted to working on data on the INSPECTr platform only.	Yes
13	All AI systems must seek to adjust existing models for bias to the full extent feasible, e.g., available adjustment data.	Design team to communicate known bias in datasets to LEAs and to identify adjustments made.	Models are adjustable through weights	Yes

17	All AI systems (including systems labelling events and objects) must provide information on errors (e.g., false positives, false negatives) and other weaknesses (e.g., poorer performance on particular groups) in the model outputs to inform LEA decision making.	AI outputs accompanied by clear explanations on their limitations.	Probabilities will be provided to the users rather than definitive answers. Weaknesses of the models will be disclosed in the documentation.	Yes
19	Design teams to consider feasibility of 'masking' certain features in AI system outputs to assist LEAs with understanding the impact of different factors/features in the AI output.	AI outputs based on composite information to provide LEAs the capacity to remove individual factors so as to observe impact.	Covered by documentation material	Yes
20	Design teams to consider whether AI system outputs can be communicated to LEAs through a harmonised approach, without affecting accuracy of information communicated.	Various AI outputs communicated in harmonised way (to extent possible).	Documentation material	Yes
23*	If they are more understandable, tools could present results confidences rather than a definitive answer to provide a more accurate picture to end-users.		In most cases, probabilities are provided rather than definitive answers	Yes

24*	Training materials need to give end-users an adequate understanding of the tools, and so it is essential that it is communicated and understood what the tools can do, what the tools are intended for, and what the tools cannot do.		Guidance on the limitations of the technology will be included in the documentation material	Yes
25*	Project tools must facilitate categorisation of categories of data-subject (e.g., suspect, criminal, victim, witness, etc.).		Categories of data-subject are not taken into account, only statistics related to the categories.	Partially, as compliance not possible but also does not impact on the subject of this requirement.

Component Number	Component's Name	Component's Acronym	Related Task	Description	Owner
20	Widgets & Analytics Windows	GRELLI	T5.1	Generic reusable, embeddable lightweight interactive investigative widgets	EBOS

ELS REQUIREMENTS vs INSPECTr COMPONENTS			Details of fulfilment	Requirement completed? (yes/no)
No	ELS Requirement's description	Measurement - Verification Action		

24*	Training materials need to give end-users an adequate understanding of the tools, and so it is essential that it is communicated and understood what the tools can do, what the tools are intended for, and what the tools cannot do.		Guidance on the limitations of the technology will be included in the documentation material	Yes
-----	---	--	--	-----

Component Number	Component's Name	Component's Acronym	Related Task	Description	Owner
21	Graphical Query Engine	GQE	T5.2	Launch automatic investigative tools using a visual or graphical prog. environment	PHS

ELS REQUIREMENTS vs INSPECTr COMPONENTS			Details of fulfilment	Requirement completed? (yes/no)
No	ELS Requirement's description	Measurement - Verification Action		
2	Rules engine should be accompanied by clear guidance on its limitations, concerning the varied nature of legal systems, the evolving nature of law, including case law.	Information on rules engine limitations embedded into technology.	As the GQE is only a sequence of the other components, this is fulfilled by the fulfilment of other technologies	Yes

24*	Training materials need to give end-users an adequate understanding of the tools, and so it is essential that it is communicated and understood what the tools can do, what the tools are intended for, and what the tools cannot do.		Guidance on the limitations of the technology will be included in the documentation material	Yes
-----	---	--	--	-----

Component Number	Component's Name	Component's Acronym	Related Task	Description	Owner
22	Toolbox: Relational Navigator	tRN	T5.3	Ability to navigate interconnections across datasets based on SIREN	SIREN

ELS REQUIREMENTS vs INSPECTr COMPONENTS			Details of fulfilment	Requirement completed? (yes/no)
No	ELS Requirement's description	Measurement - Verification Action		
2	Rules engine should be accompanied by clear guidance on its limitations, concerning the varied nature of legal systems, the evolving nature of law, including case law.	Information on rules engine limitations embedded into technology.	Guidance on the limitations of the technology will be included in the documentation material	Yes

24*	Training materials need to give end-users an adequate understanding of the tools, and so it is essential that it is communicated and understood what the tools can do, what the tools are intended for, and what the tools cannot do.		Guidance on the limitations of the technology will be included in the documentation material	Yes
25*	Project tools must facilitate categorisation of categories of data-subject (e.g., suspect, criminal, victim, witness, etc.).		Data can be categorised by subject using an Analyzer.	Yes

Component Number	Component's Name	Component's Acronym	Related Task	Description	Owner
23	Open-Source Case Management System	CMS	T5.4	Graphical UI providing users and users' rights management, controlled access to investigations data and visualisation through the dashboard, widgets and other components.	PHS

ELS REQUIREMENTS vs INSPECTr COMPONENTS	Details of fulfilment	Requirement completed?
--	------------------------------	-------------------------------

No	ELS Requirement's description	Measurement - Verification Action		(yes/no)
2	Rules engine should be accompanied by clear guidance on its limitations, concerning the varied nature of legal systems, the evolving nature of law, including case law.	Information on rules engine limitations embedded into technology.	Guidance on the limitations of the technology will be included in the documentation material	Yes
11	LEAs should be able to delete their data across the INSPECTr Platform and Tools with relative ease. This means that developers should ensure that data residue is avoided on the Platform and in Tools.	LEA able to delete their INSPECTr data across the Platform in a limited number of steps.	Features provided by CMS : case archiving, case deletion for users with case management rights	Yes
12	The design team in consultation with LEAs should consider the automated deletion of data, with prompts alerting LEAs to proactively continue storage. · This is advised especially for INSPECTr network data that has been obscured, such as ‘queries’ between Member State LEAs.	Automated deletion time frames established, requiring investigator to proactively choose continued storage.	Cache cleaning based on cron-jobs process	Yes
24*	Training materials need to give end-users an adequate understanding of the tools, and so it is essential that it is communicated and understood what the tools can do, what the tools are intended for, and what the tools cannot do.		Guidance on the limitations of the technology will be included in the documentation material	Yes

25*	Project tools must facilitate categorisation of categories of data-subject (e.g., suspect, criminal, victim, witness, etc.).		Whilst the categories of data-subjects can be viewed through data present in the CMS, the technology itself can only categorise end-users.	Yes
-----	--	--	--	-----

As noted above, as INSPECTr is a research project, we cannot expect the results to be fully compliant with all requirements imposed on them. However, as is shown above, most of the INSPECTr technologies have fulfilled the vast majority of ELS requirements that were developed in the project. As such, the INSPECTr technologies have gone a significant way toward being seen as ‘trustworthy’ or ‘responsible’ from the perspective of ethical AI. There is still some research and development work to be completed, or explored, to fulfil all the requirements for all tools. However, this is expected to be completed before the tools are made available to LEAs or other potential end-users. In any case, the technologies have been enhanced from the ethical, legal, and societal perspective than if these requirements, and WP8, were not developed and implemented. As such, the work done toward developing INSPECTr as a platform of ‘trustworthy’ or ‘responsible’ AI technologies is hugely beneficial for enabling their future use.

5 Horizon scanning and sensitization efforts

Horizon scanning is a process of researching emerging issues that could impact on a particular area. In INSPECTr, TRI examined many sources to evaluate whether potential issues could impact on either the INSPECTr technologies or project. Where issues were identified that could impact on the project or technologies, these were raised and discussed with relevant partners. In the first half of the project, this resulted in workshops on ethical AI, online data collection, and gender and AI. Having covered many cross-consortium issues earlier in the project, the horizon scanning and sensitisation efforts in the second half of the project were more nuanced and focussed in specific areas, sometimes with a specific partner. In any case, horizon scanning has been a beneficial task for the INSPECTr project to keep up-to-date with new developments affecting law enforcement and AI.

5.1 Post-project exploitation risks

From the start of the project, TRI and the EAB have raised and discussed concerns regarding risks that could be created by the INSPECTr technologies being used by LEAs in future. The very nature of policing means that people rights can be infringed through investigations into people's private lives and also impact on their liberty through arrests. These risks are generally acceptable to society, where they are taken in lawful ways and for legitimate reasons. However, providing powerful technologies to LEAs, especially ones that are intended to speed up their work, could mean that their work would result in more rights being infringed upon, even where this is lawful and legitimate. It is debatable whether this is ethically justifiable. However, following discussions at WP8 meetings in INSPECTr, partners agreed that this could be justified where tools like the INSPECTr platform are subject to strong and effective safeguards.

Potentially a more impactful consideration is that there are many examples of LEAs exceeding their powers, whether by a deliberate policy choice to act in an illegitimate way (e.g., engaging in mass surveillance), the exceeding of lawful limits in pursuit of a legitimate aim at all costs (e.g., an excessive examination of a suspect's private life in the hope of finding a missing person), or merely not considering the full implications of their activities (e.g., over policing of ethnically diverse areas). Even if the INSPECTr platform could be considered as perfectly 'trustworthy' or 'responsible' from the perspective of AI ethics, it could still be misused for the reasons mentioned or others. As such, there is an imperative to recognize risks of exploitation of the INSPECTr platform to LEAs who exceed their powers.

The nature of INSPECTr as an European Commission-funded research project means that partners are under an obligation to engage in 'exploitation' of the project results, whether using them in future projects, products, services, or standardization activities. However, there is little guidance available from the European Commission about how exploitation should be approached where there are ethics concerns about how a technology could be used. As such, there is a clear risk that a powerful technology, like the INSPECTr platform (or parts of it), could be exploited without clear safeguards.

These issues are something that has been recognized and considered in the INSPECTr project. TRI has raised this issue at WP8 meeting, and also engaged in discussions with partners who provide their technologies to others (e.g., CCI, SIREN, and ILS) about how they deal with providing technologies to potentially risky organisations. As a result of raising these issues, and discussing them across the INSPECTr project, TRI developed the 'Know Your Customer' Exploitation Risk Assessment that is included in *D8.8: Guide on privacy and ethics-by-design in law enforcement technology*. This work was developed to take account of potential risks and provide a practical way of dealing with them from the position of a technology provider who might engage in sales where there could be potential risks raised by certain clients.

5.2 Policy proposals regarding end-to-end encryption

The EU² and other governments³ have recently made policy announcements to deal with the use of end-to-end encrypted services by criminal, especially criminals who engage in child abuse online and in-person. End-to-end encryption is a way of keeping communication between two or more parties secure such that only those parties can view the content of those communications. For example, popular messaging apps like WhatsApp and Signal include end-to-end encryption for messages (though back-ups might be treated differently).

These policy announcements raise the prospect of outlawing end-to-end encryption as it stands by requiring a ‘backdoor’ that would allow LEAs and intelligence agencies access to encrypted services, or requiring development of some other alternative to end-to-end encryption. Primarily, these policy announcements are focused on how end-to-end encryption could frustrate investigations into child sexual abuse and exploitation and terrorism. As these two areas are use-cases for INSPECTr, TRI examined and considered the implications of these proposals for the project technologies and their future use.

As INSPECTr includes technologies that analyse data from sources not generally wholly subject to encryption (e.g., devices such as mobile phones), and the project is not focused on encryption as a research area, TRI determined that whilst this area was worthy of horizon scanning, it was not a subject that the consortium needed to be sensitized to as a priority.

5.3 Anonymisation of sensitive personal data

Due to the nature of LEA data being especially sensitive, it can take significant work to fulfil all the obligations needed to adequately safeguard personal data in order that such data could be used in a research project. However, where personal data is successfully anonymized, such data falls outside of data protection law (though ethical concerns are still prevalent).

Having recognized the difficulties of completing data protection impact assessments for access to LEA data for testing of INSPECTr technologies (see *D8.4: Third Report on Ethical Governance*), TRI began horizon scanning on the potential for anonymization techniques to be used in order to more easily facilitate access to LEA data. TRI researched various data minimization techniques and how these could be judged for the quality of data minimization, as well as understanding how to accurately define anonymous data under data protection law. This coincided with discussing anonymisation with both technical and LEA partners who were interested in anonymization as a way to more easily access and process closed case data.

As datasets vary widely, and only certain partners were concerned with potentially anonymized closed case data, TRI determined that it would be best to hold discussions on the potential for using anonymization techniques with the technical and LEA partners most interested in exploring these options and centre these discussions on the data being considered. The information of most interest to relevant technical partners from closed case files included data categories that are used to formalize data collected during investigations for analysis by technologies. These categories were of interest to ensure that the INSPECTr technologies can comprehend the data structures used by different organisations.

Whilst anonymization can lower the burden needed to process sensitive data, it can involve significant efforts to successfully anonymise personal data in the first place. Whilst discussing this issue, it became apparent that,

² Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse, COM/2022/209 final, 11th May 2022. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A209%3AFIN&qid=1652451192472>

³ UK Government and others, ‘International statement: End-to-end encryption and public safety’, Gov.uk, 16 January 2023. Available at: <https://www.gov.uk/government/publications/international-statement-end-to-end-encryption-and-public-safety>

whilst taking steps to avoid security concerns, much of the information needed by relevant technical partners could simply be explained by LEAs during discussions of their needs. As such, a detailed analysis of possible anonymisation techniques and the efficacy of those for the proposed data were not needed as the implementation of anonymisation techniques was unlikely to be proportionate to the required efforts. However, the knowledge gained by TRI during this process was still useful for providing advice of anonymisation efforts required for other datasets during the project. This knowledge was also used by TRI to contribute to standardisation efforts regarding privacy enhancement through de-identification of personal data.

6 Conclusions

This deliverable assesses the INSPECTr technologies in terms of their compliance with the ethical, legal, and societal requirements determined in *D8.5: Ethical, Legal and Social requirements for the INSPECTr platform and tools*. Each tool is examined in turn and, whilst there are some gaps, the INSPECTr technologies have made great progress toward being seen as ‘trustworthy’ or ‘responsible’ from the perspective of AI ethics. Further, this deliverable also outlines three horizon scanning and sensitisation efforts: post-project exploitation risks; policy proposals regarding end-to-end encryption; anonymisation of sensitive personal data.

Overall, the process of defining and implementing ethical, legal, and societal requirements in INSPECTr has been positive. The requirements themselves were created in a partially collaboratively way, and their implementation took a somewhat co-design approach through the Ethics Manager and technical partners discussing the requirements, the concepts behind them, and the technical possibilities for meeting them, which has been enlightening for all involved. The level of compliance with the requirements has generally been good, with most requirements being fulfilled for most technologies. As has been mentioned, the outputs from INSPECTr are research results and not products, and so we would not expect all technologies to meet all requirements. Recognising this, the ethical approach taken to technology design in INSPECTr has been beneficial, as it has resulted in technical partners being able to consider ethical aspects to their work beyond the narrow descriptions of their technical tasks, thereby creating technologies that are more compliant with ethical, legal, and societal standards than they would otherwise have been had this work not been included in the INSPECTr project.