INSPECTr

# Intelligence Network & Secure Platform for Evidence Correlation and Transfer

# D8.3 Second Report on Ethical Governance

## Document Summary Information

| | | | |
|---|---|---|---|
| **Grant Agreement No** | 833276 | **Acronym** | INSPECTr |
| **Full Title** | **I**ntelligence **N**etwork & **S**ecure **P**latform for **E**vidence **C**orrelation and **Tr**ansfer | | |
| **Start Date** | 01/09/2019 | **Duration** | 42 months |
| **Project URL** | https://www.inspectr-project.eu | | |
| **Deliverable** | D8.3 Second report on Ethical Governance | | |
| **Work Package** | WP 8 | | |
| **Contractual due date** | 31/08/2021 | **Actual submission date** | 31/08/2021 |
| **Nature** | R | **Dissemination Level** | PU |
| **Lead Beneficiary** | TRI | | |
| **Responsible Author** | Dr. Joshua Hughes | | |
| **Contributions from** | Dr. David Barnard Wills, Dr. Leanne Cochrane, David Wright | | |

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Grant Agreement No 833276.

### *Revision history (including peer reviewing & quality control)*

| Version | Issue Date | % Complete | Changes | Contributor(s) |
|---|---|---|---|---|
| v.0.1 | 11.01.21 | 0 | Initial Deliverable Structure | Leanne Cochrane |
| v.0.2 | 13.01.21 | | Internal review | David Barnard-Wills |
| v0.3 | 14.01.21 | | Amends following internal review for circulation to peer reviewers | Leanne Cochrane |
| v0.4 | 10.02.21 | | Peer review | Fabrizio Turchi |
| v0.5 | 12.02.21 | | Peer review | Toomas Plaado |
| v0.6 | 22.02.21 | | EAB review | Daragh O Brien |
| v1.0 | 25.02.21 | 100 | Revision following peer review and EAB review | Joshua Hughes |
| V1.1 | 01.06.21 | | Subsequent deliverable structure | Joshua Hughes |
| V1.2 | 07.07.21 | | Updates | Joshua Hughes |
| V1.3 | 12.07.21 | | Internal review | David Barnard-Wills |
| V1.4 | 10.08.21 | | Update following internal peer-review | Joshua Hughes |
| V2.0 | 25.08.21 | 100 | Update following UCD DPO review | 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*

# Table of Contents

1 Introduction .....5

1.1 Mapping INSPECTr Outputs .....5

1.2 Deliverable Overview and Report Structure .....6

2 The Ethical Management Processes .....7

2.1 Standing Processes: Weekly, Monthly or Quarterly .....7

2.1.1 Internal TRI Review Meetings – Weekly and Monthly .....7

2.1.2 INSPECTr Meetings - Monthly .....7

2.1.3 Ethics Advisory Board Quarterly Meetings .....8

2.2 Ad Hoc Processes: In Response to Project Need .....8

2.2.1 INSPECTr Law Enforcement Authority Steering Group ('LSG') Monthly Project Meetings .....8

2.2.2 INSPECTr Technical Meetings .....9

2.2.3 TRI Discussion Requests with Individual Partners .....9

2.2.4 Ethics Webinars and Partner Dialogues .....9

2.3 Communications Channels: Continuous .....10

2.3.1 Only Office Platform .....11

2.3.2 Rocket Chat #Ethics Thread .....12

2.3.3 Individual Partner Contact with Ethics Manager – Email, Telephone, Teams, GoToMeeting, Skype and Private Message. .....12

2.3.4 Ethics reviews of deliverables .....12

3 Tools Used to Identify and Monitor Ethical Issues .....13

3.1 Data Management Plan .....13

3.2 Data Protection Impact Assessments ('DPIAs') .....13

3.3 Incidental Findings Policy & Log .....14

3.4 Non-EU Transfer of Personal Data Log .....14

3.5 ILS INSPECTr Risk Assessment Tool .....14

3.6 Legal Basis for Processing Personal Data .....14

3.7 TRI 'Touchpoint Table' for Ethical Issues .....16

3.7.1 Personal Data Processing Timeline .....16

4 Ethical Issues Experienced during M18-M24 of the INSPECTr Project .....17

4.1 Application to use human participants submitted to UCD Ethics Committee .....17

4.2 Processor-Controller Agreement template for LEA use of Living Labs .....18

4.3 International Data Transfers .....19

4.3.1 Transfers of Personal Data to UK-based partners .....19

4.3.2 Transfers of Personal Data to the US .....20

4.4 The potential impact of the EU's proposed AI regulation .....21

4.5 Anonymisation of real case data, and of real mobile phone data .....21

4.5.1 Exploring the use of real and realistic data by Consiglio Nazionale Delle Richerche .....21

4.5.2 Anonymising datasets by Gendarmerie Nationale .....22

4.6 Ethics and Privacy-by-design .....23

5 Conclusions .....24

6 Annex 1: INSPECTr Incidental Findings Policy .....25

## List of Figures

Figure 1: Screenshot from INSPECTr OnlyOffice 'Ethics' subfolder (at 10 August 2021) .................................... 11
Figure 2: Screenshot from Rocket Chat #Ethics Thread Heading ......................................................................... 12
Figure 3: Screenshot of Headings Used in INSPECTr's 'TRI TouchPoint Table' .................................................... 16
Figure 1: INSPECTr Reporting Process for Suspected Incidental Findings .......................................................... 32

## List of Tables

Table 1: Adherence to INSPECTr GA Deliverable & Tasks Descriptions .................................................................5

## Glossary of terms and abbreviations used

| Abbreviation / Term | Description |
|---|---|
| CCI | UCD Centre for Cybersecurity and Cybercrime Investigation |
| DMP | Data Management Plan |
| DPA | Data Protection Authority |
| DPIA | Data Protection Impact Assessment |
| DPO | Data Protection Officer |
| EAB | Ethics Advisory Board |
| EC | European Commission |
| EDPS | European Data Protection Supervisor |
| GDPR | General Data Protection Regulation |
| LEA | Law Enforcement Authority |
| LED | Law Enforcement Directive |
| LIA | Legitimate Interests Assessment |
| LSG | Law Enforcement Authority Steering Group |
| NLP | Natural Language Processing |
| POPD | Processing of Personal Data |
| TRI | Trilateral Research |
| UCD | University College Dublin |
| WP | Work Package |

# 1 Introduction

The aim of this deliverable is to document the ethical management processes and any ethical issues experienced between months 18 and 24. This is an updated version of the report. The final version to be submitted at month 42 will include a guide on results exploitation and use after the end of the project.

## 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** | | | |
| *D8.3 Second Report on Ethical Governance* | *A report documenting the ethical management processes and any ethical issues experienced during the project.* | *Sections 2, 3 and 4.* | *Sections 2 and 3 document the ethics management processes and tools used within these processes.*<br>*Section 4 documents the ethical issues experienced between months 18 and 24 of the project.* |
| **TASKS** | | | |
| *ST8.1.1 Research Ethics* | *Commit to responsible research and innovation, research ethics…Set up a regular ethics review process including an ethics review panel. Identify and assess any ethical issues that might arise from each of INSPECTr's activities and deliverables and define measures to be taken in the case of ethical issues…Manage relationships with relevant ethics stakeholders.* | *Sections 2, 3 and 4.* | *Sections 2 and 3 document the ethics management processes and tools used within these processes.*<br>*Section 4 documents the ethical issues experienced between months 18 and 24 of the project.* |

## 1.2 Deliverable Overview and Report Structure

This deliverable has three main sections.

Section 2 sets out the INSPECTr ethical management processes. This includes standing processes and ad hoc processes as well as INSPECTr ethics communication channels.

Section 3 sets out seven (7) tools used by the INSPECTr project to identify and monitor ethics issues in the project. These tools provide a foundation for ethical discussions during the processes outlined in Section 2.

The above sections have been reviewed and updated since submission of the first report. This includes an update of meeting dates, and an update on how the ethics management process, and tools used for it, have been adapted to the needs of the project over months 18-24.

Section 4 sets out the main ethical issues experienced by Trilateral Research Ltd (TRI) between month 18 when the first report was submitted, and month 24 when this report is submitted.

# 2 The Ethical Management Processes

This section sets out the ethical governance processes used by TRI within the project. The section is divided into standing processes which occur at a set regular date and time and ad hoc processes, which may occur regularly but are engaged by the ethics team as needed. The final subsection outlines the main communication tools used by the Ethics Manager, Trilateral Research Ltd. (TRI), and the other project partners to discuss and share information on ethical issues within the project.

This is the internal ethics management process within the project and is complemented by the EC's own external ethical review process.

## 2.1 Standing Processes: Weekly, Monthly or Quarterly

There are three types of standing process relevant to the discussion and management of ethical issues within the project: (i) meetings that are internal to partner TRI only; (ii) meetings between TRI and other INSPECTr partners; (iii) meetings between TRI and the independent Ethics Advisory Board (EAB).

### 2.1.1 Internal TRI Review Meetings – Weekly and Monthly

The TRI Ethics Manager reviews the project on a weekly basis with colleagues. Within TRI, there are then monthly meetings between the TRI project team (i.e., TRI staff working across WP6, WP7 and WP8), as well as monthly project meetings between the project lead, the lead's line manager and the Director. These meetings cover all aspects of TRI's work in INSPECTr but focus predominantly on WP8 ethics management as it is the largest responsibility attributed to TRI within the Grant Agreement.

### 2.1.2 INSPECTr Meetings - Monthly

The INSPECTr Coordinating Partner CCI, hosts a monthly consortium meeting, typically every first Tuesday of the month for two hours. During this meeting, the TRI Ethics Manager presents a PowerPoint to update partners on the WP8 ethics activities over the past month and looks forward to the intended activities over the next 30-day and 90-day periods. Outstanding queries are sometimes raised with partners by the Ethics Manager at this meeting and partners can ask questions of the ethics lead. Note that the March and April 2021 meetings were combined into a Project General Assembly meeting; however, discussion of ethics issues was still able to occur. Points relevant to ethics governance were also discussed at the project's Mid-term Review. The following monthly consortium meetings have been attended by the TRI Ethics Manager, with associated WP8 presentations delivered between months 18 and 24:

- 2nd March 2021
- 15-16th April 2021 (Project General Assembly)
- 1st June 2021
- 2nd July 2021 (Mid-Term Review Meeting)
- 10th August 2021

Since November 2020, following the second ethics check, the TRI Ethics Manager has established monthly WP8 meetings with other WP leads. These meetings are scheduled for one on the last Monday of the month to allow for a fuller discussion of the ethics issues within the project. The EAB chair (i.e., Castlebridge) and EAB project partners (i.e., RUG) are also invited and encouraged to attend this meeting. The WP8 monthly meeting deliberately falls every quarter on the same day as the EAB quarterly meetings. To date, the following WP8 monthly meetings have been held between months 18 and 24 (an August meeting was cancelled due to holidays):

- 22 March 2021
- 26 April 2021
- 24 May 2021
- 28 June 2021
- 26 July 2021

### 2.1.3 Ethics Advisory Board Quarterly Meetings

Since October 2020, following the second ethics check, the EAB has established standing quarterly EAB meetings to discuss and oversee ethical issues arising from the INSPECTr project. These meetings are held on the last Monday of the month every quarter. The TRI Ethics Manager attends these meetings. The EAB Chair liaises with the TRI Ethics Manager to identify any priority issues for discussion. Prior to the quarterly meetings, the EAB met to review the ethics requirements (WP9) deliverables on an ad hoc basis.

To date, the following EAB meetings attended by the TRI Ethics Manager have been held between months 18 and 24:

- 26 April 2021
- 26 July 2021

## 2.2 Ad Hoc Processes: In Response to Project Need

### 2.2.1 INSPECTr Law Enforcement Authority Steering Group (‘LSG’) Monthly Project Meetings

While there are regular Law Enforcement Authority Steering Group (‘LSG’) meetings, the TRI Ethics Manager can request, or can be requested, to attend these meetings from the Coordinating Team on an as-needed basis. This will occur where the TRI Ethics Manager identifies a need to discuss ethics issues directly and more fully with the law enforcement authorities (LEAs) who may not always attend the monthly consortium meetings, or there is an ethics-related issue that the Coordinating Team want to bring to the attention of the LEA partners. Between months 18 and 24, these discussions have focussed on: advising LEA partners on the completion of data protection impact assessments (DPIAs) ahead of carrying out testing in the Living Labs (LLs), this has also involved TRI communicating directly with LEA Data Protection Officers (DPOs) to monitor progress of DPIAs; discussing the expected data processing relationships between LEAs and technical partners for the LLs in order to develop a template Data Controller-Processor contract for LEA partners to use to ensure consistency across contracts. To date, the following LSGs have been attended by the TRI Ethics Manager between months 18 and 24:

- 12 May 2021
- 9 June 2021
- 7th July 2021
- 11th August 2021

### 2.2.2 INSPECTr Technical Meetings

During the early stages of the project the main consortium meetings were technical meetings aimed at defining further the INSPECTr requirements, and, general project meetings, and WP8 meetings, were not happening as regularly as they are now. Due to the existence of multiple other avenues for engagement, the TRI Ethics Manager does not now routinely attend the ongoing weekly technical meetings, nor has there been any attendance between months 18 and 24. Rather, technical partners have attended specific WP8 meetings to discuss ethical issues, and the Ethics Manager can attend technical meetings where requested. The TRI Ethics Manager has requested that ethical representation be included in any technical demonstrations held by project partners.

### 2.2.3 TRI Discussion Requests with Individual Partners

A core way the TRI Ethics Manager liaises with partners to encourage and ensure ethical commitments are considered and adhered to within the project is through one-to-one communication with partners. This is a weekly activity for the TRI Ethics Manager and occurs through email, telephone, Skype, Teams, and GoToMeeting channels as needed.

### 2.2.4 Ethics Webinars and Partner Dialogues

The TRI Ethics Manager has organised a number of ethics webinars and in-depth ‘partner dialogues’ (referred to as ‘workshops’ where external expertise has been included), to assist partners in the fulfilment of their ethics commitments. The following webinars, dialogues or workshops have occurred between months 18-24:

- **09.06.2021, Workshop: Gender and AI in the INSPECTr Project and Platform**
    - <u>Agenda:</u>

1) Issues for IT systems in general that arise from common assumptions about the nature of gender as a concept or category.
    a. How might this manifest in INSPECTr?
    b. Does the evidence representation and exchange format do anything with gender?
    c. Do any of the connectivity adaptors or tools, open-source investigative tools do anything with gender? If so, then do they assume a binary male/female categorisation?
2) Limited gender perspectives in design team.
    a. How might this manifest in INSPECTr?
    b. What is the gender balance of the end users?
    c. How will we cover a mix of genders through the capture of training needs and recruitment/involvement in LEA capacity building programme (T6.1)
3) Missing data with a gender skew
    a. How might this manifest in INSPECTr?
    b. Would the work being done to support the development of crime prediction approaches (T4.5) work for the types of violence disproportionally affecting women? Could they work for types of crime that we know are under-reported (e.g. domestic violence, rape and sexual assault?). If we are just creating tools and infrastructure that LEAs can then use with their own data, are we providing any advice or guidance on how they should deal with gender data issues?
    c. Might there be any gender gaps in the information available through connectivity adaptors/API from existing opens source investigative tools/information sources? (T3.2)
    d. Do our use cases cover a range of crime or investigation types that covers those types of crimes or investigations that disproportionately affect women?
    e. Can we document our datasets? Have we assessed any of our datasets for under-representation of different gender identities?

4) Gender biases in machine learning
    a. How might this manifest in INSPECTr?
    b. Have we considered the impact that gendered embeddings might impact Natural Language Processing (NLP) models (considering how they might be used in practice)?
    c. Do the NLP tools perform better or worse on data associated with different genders (e.g. gender of authors, gender of subjects of a text)?
    d. Are there observable changes in sentiment analysis when the only difference are words that correspond to gender?
    e. Have we considered ways in which we might mitigate gender bias in NLP as used in INSPECTr
    f. T4.4 is developing computer vision applications including categorisation/classification
    g. Do computer vision applications perform better/worse on different genders?
    h. How have the gender bias issues of emotion recognition tools been considered?
5) 5) Gender attribution / Recognition
    a. How might this manifest in INSPECTr
    b. Do any of the computer vision applications do gender attribution/classification?
    c. Do they need to? Is gender attribution necessary for an identified functionality with evidence that this functionality is needed? Can we avoid implementing automated gender attribution?
    d. Is gender being used as a proxy/approximate variable/categorisation anywhere in INSPECTr where a more precise variable might be used instead?
6) Formally discriminatory effects on the basis of gender
    a. How might this manifest in INSPECTr?
    b. How are we ensuring that recruitment to INSPECTr training activities is gender-neutral?
7) Different impacts in the real-world on the basis of gender.
    a. Are we including any assessment or evaluation relation to gender in the evaluation of INSPECTr platform? Can we identify what might be appropriate questions to ask?
    b. How might the deployment of the INSPECTr tools in the world have differential impacts for people of different genders?

Format: Live two-hour Teams meeting

Attendance: Allison Gardner (external);[1] Castlebridge; CCI; LSP; EPBG; GN; TRI; VLTN; IGPR; ILS; eBOS; UCD.

## 2.3 Communications Channels: Continuous

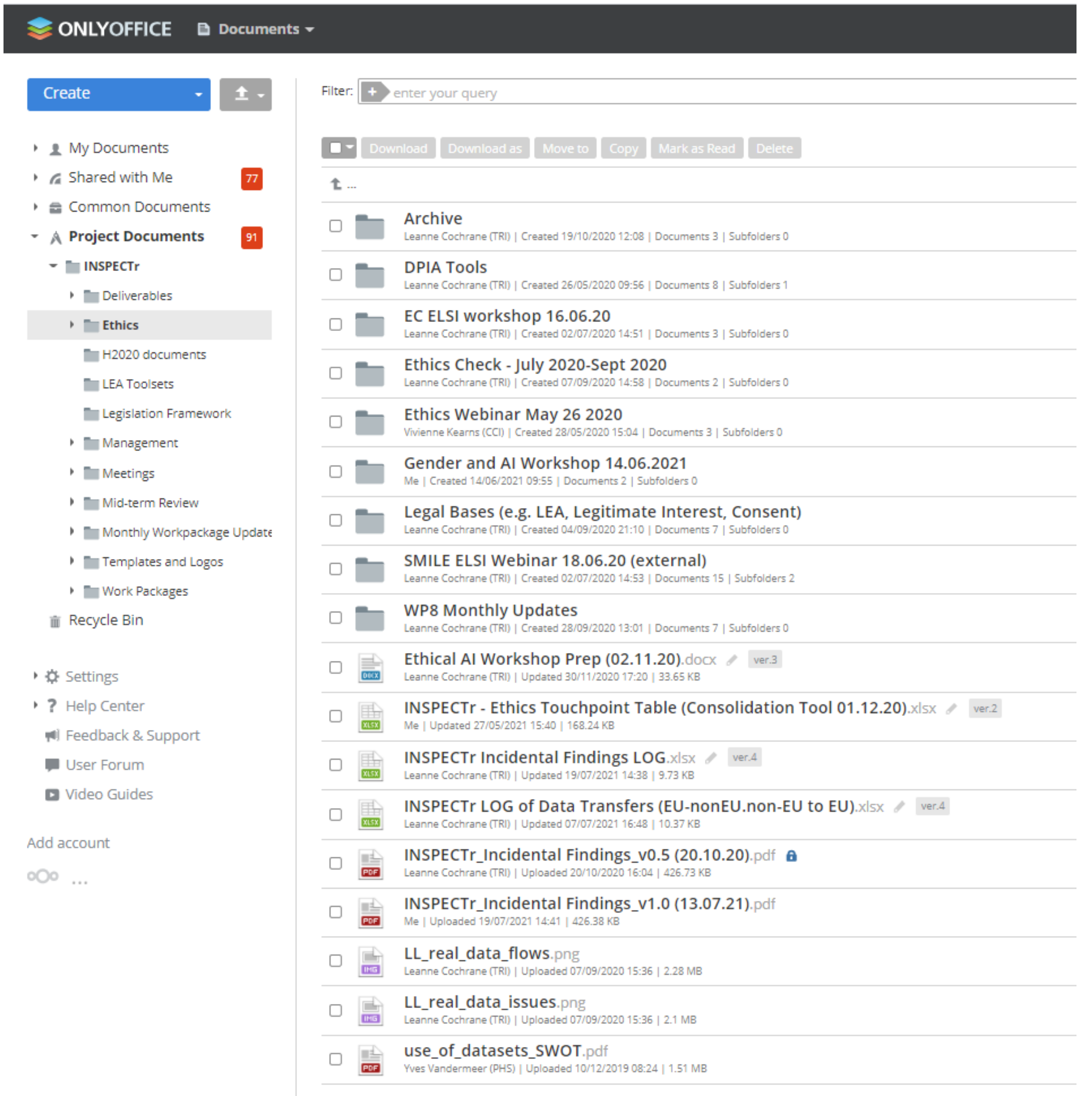
There are three core communications channels used by the TRI Ethics Manager to communicate with project partners. At the project level, the most formal channel is the project OnlyOffice platform. This is followed by the less formal RocketChat #Ethics thread. On an individual level, the TRI Ethics Manager regularly communicates with partners through email, telephone, Skype, Teams and GoToMeeting. The nature of ethics communications on the OnlyOffice Platform and RocketChat are described below.

[1] Dr Gardner provided her name for this deliverable on the condition that the following recommendations are included: Technologies such as emotion detectors are not a proven technology, and so should not be included in the INSPECTr platform at the end of the project; NLP developed from some of the corpuses with known inherent biases that are intended to be used by INSPECTr partners (e.g. Wikipedia) would have biased effects on the resulting technologies. Since this discussion, technical partners have decided not to pursue deployment of the emotion detection tool (see D4.6), and the impact of some corpora datasets have been reviewed and found no significant biases (see D4.4).

### 2.3.1 Only Office Platform

Ethics deliverables, tools and working documents are primarily shared with partners and the EAB through the OnlyOffice platform established by CCI. All ethics deliverables are stored in the main deliverables folder. Otherwise, a specific 'Ethics' folder is used by the TRI Ethics Manager to collate information viewable by all partners on issues such as: partner legal basis for processing personal data, European Commission (EC) ethics check responses, ethics training tools, and workshop notes. The project 'Incidental Findings Policy' and 'Log' as well as the project 'Data Transfer Log' are also stored and available to partners in this folder. Ahead of WP8 meetings, WP leads are invited to review the data management plan, log of international data transfers, the log of incidental findings, and the Ethics TouchPoint Table in case any updates need to be recorded.[2] Any updates are then discussed during the meeting. See Figure 1 below for a screenshot of the folder contents – the working documents within the folder are confidential to the project.

Figure 1: Screenshot from INSPECTr OnlyOffice 'Ethics' subfolder (at 10 August 2021)



□ Archive
Leanne Cochrane (TRI) | Created 19/10/2020 12:08 | Documents 3 | Subfolders 0

□ DPIA Tools
Leanne Cochrane (TRI) | Created 26/05/2020 09:56 | Documents 8 | Subfolders 1

□ EC ELSI workshop 16.06.20
Leanne Cochrane (TRI) | Created 02/07/2020 14:51 | Documents 3 | Subfolders 0

□ Ethics Check - July 2020-Sept 2020
Leanne Cochrane (TRI) | Created 07/09/2020 14:58 | Documents 2 | Subfolders 0

□ Ethics Webinar May 26 2020
Vivienne Kearns (CCI) | Created 28/05/2020 15:04 | Documents 3 | Subfolders 0

□ Gender and AI Workshop 14.06.2021
Me | Created 14/06/2021 09:55 | Documents 2 | Subfolders 0

□ Legal Bases (e.g. LEA, Legitimate Interest, Consent)
Leanne Cochrane (TRI) | Created 04/09/2020 21:10 | Documents 7 | Subfolders 0

□ SMILE ELSI Webinar 18.06.20 (external)
Leanne Cochrane (TRI) | Created 02/07/2020 14:53 | Documents 15 | Subfolders 2

□ WP8 Monthly Updates
Leanne Cochrane (TRI) | Created 28/09/2020 13:01 | Documents 7 | Subfolders 0

□ Ethical AI Workshop Prep (02.11.20).docx ver.3
Leanne Cochrane (TRI) | Updated 30/11/2020 17:20 | 33.65 KB

□ INSPECTr - Ethics Touchpoint Table (Consolidation Tool 01.12.20).xlsx ver.2
Me | Updated 27/05/2021 15:40 | 168.24 KB

□ INSPECTr Incidental Findings LOG.xlsx ver.4
Leanne Cochrane (TRI) | Updated 19/07/2021 14:38 | 9.73 KB

□ INSPECTr LOG of Data Transfers (EU-nonEU.non-EU to EU).xlsx ver.4
Leanne Cochrane (TRI) | Updated 07/07/2021 16:48 | 10.37 KB

□ INSPECTr_Incidental Findings_v0.5 (20.10.20).pdf
Leanne Cochrane (TRI) | Uploaded 20/10/2020 16:04 | 426.73 KB

□ INSPECTr_Incidental Findings_v1.0 (13.07.21).pdf
Me | Uploaded 19/07/2021 14:41 | 426.38 KB

□ LL_real_data_flows.png
Leanne Cochrane (TRI) | Uploaded 07/09/2020 15:36 | 2.28 MB

□ LL_real_data_issues.png
Leanne Cochrane (TRI) | Uploaded 07/09/2020 15:36 | 2.1 MB

□ use_of_datasets_SWOT.pdf
Yves Vandermeer (PHS) | Uploaded 10/12/2019 08:24 | 1.51 MB

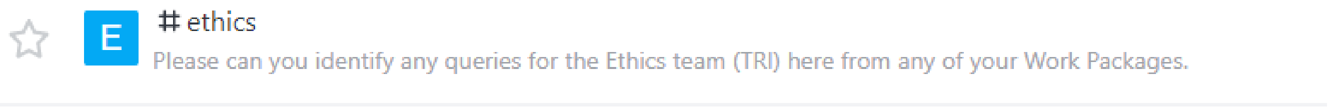
[2] The Ethics TouchPoint Table is updated where there are any updates on processing of personal data, online personal data, international data transfers, AI modelling/discrimination risks, human participation, profiling or surveillance, or other ethics risks not previously mentioned.

The TRI Ethics Manager also uses the OnlyOffice platform ‘Discussion’ threads to communicate to partners about the uploaded ethics documents and forthcoming events.

### 2.3.2 Rocket Chat #Ethics Thread

INSPECTr partners use RocketChat to communicate on a more informal basis.  A distinct #Ethics Thread exists for ethics specific (WP8) communication, which is open to all partners to view and contribute.  Partners have been encouraged to post ethics queries to this thread. This forum is however, more commonly used to share information, such as communications around the occurrence of ethics focused webinars by other H2020 security projects, notes from attendees and data protection updates, e.g., on Brexit. The diagram on data flows within INSPECTr task T1.3, prepared by CCI for the T1.3 law enforcement authorities (LEA) data protection impact assessments (DPIAs), was also shared on this thread as a helpful visual aid for all technical and non-technical partners. See Figure 2 below for a screenshot of the thread heading – the content of the thread is confidential to the project.

Figure 2: Screenshot from Rocket Chat #Ethics Thread Heading



# ethics

Please can you identify any queries for the Ethics team (TRI) here from any of your Work Packages.

### 2.3.3 Individual Partner Contact with Ethics Manager – Email, Telephone, Teams, GoToMeeting, Skype and Private Message.

The TRI Ethics Manager sends and receives emails with individual partners regularly. Email is the preferred medium for making formal requests of partners where the issue is considered fundamental to meeting the ethics requirements of the project. Where further elaboration is necessary, Skype, Teams and GoToMeeting have all been platforms regularly used by the TRI Ethics Manager when engaging with partners.  Finally, Rocket Chat also has the option of private messaging individual partners. This is also frequently used for less formal queries with individual partners.

### 2.3.4 Ethics reviews of deliverables

The TRI Ethics Manager conducts ethics reviews of deliverables that could contain information pertaining to ethical concerns, or information on tasks that have required ethics oversight, to ensure that the issues have been dealt with properly and are presented in an appropriate way. This is in addition to peer-reviews by other partners as part of the internal process in INSPECTr for the submission of deliverables. Generally, the result of these reviews is minor modifications to the presentation of information in the deliverables. However, ethics advice given during these reviews has resulted in changes to the INSPECTr tools; for example, recommendations to present confidences with image classification tools were incorporated into the technology itself.

# 3 Tools Used to Identify and Monitor Ethical Issues

There are a number of tools used within the project to identify and track ethical issues. This section details seven (7) core INSPECTr tools, which are regularly referred to in the ethical governance processes referenced above in section 2 of the deliverable.

## 3.1 Data Management Plan

The Data Management Plan (DMP) documents the consortium's plan on the handling of research data during the project and after the end of the project. This includes what data will be collected, processed and/or generated, which methodology and standards will be applied, whether data can be shared or made open access (OA)[3] and how data will be curated and preserved in line with the H2020 Guidelines on FAIR Data Management (2016).[4] It is a project 'living' document, with the first iteration available from month 6 of the project and routinely updated since this time.

Section 2 of the DMP is especially helpful for monitoring the intentions of partners concerning research data. It provides an overview by both partner and task of the research data, including personal data, to be processed within INSPECTr. The information within section 2 is consistently harmonised with the 'TRI TouchPoint Table' (see section 3.7 below).

As mentioned above, requests concerning partner updates to the DMP is a standing item at the monthly WP8 meetings (and previously at the monthly consortium meetings). The DMP is available to and amendable by all partners on OnlyOffice, within the 'Management' subfolder. Previous substantial iterations are also stored in an 'archive' folder.

## 3.2 Data Protection Impact Assessments ('DPIAs')

Ethics Requirement No.17 (deliverable D9.15) set out TRI's assessment concerning whether a DPIA is needed for individual INSPECTr tasks. This assessment followed the guidance set out in Opinion WP248 of the Article 29 Working Party.[5] TRI advised a DPIA for INSPECTr Tasks T1.3, ST3.2.4, ST4.4.1 and ST4.4.2 and provided a comprehensive DPIA template to assist partners. At the time of writing, first drafts of DPIAs have been completed for partners AGS and BFP, and are in-progress for EPBG and IGPR, for T1.3 (Living Labs), and from partner CCI for ST3.2.4 (web scraper), ST4.4.1 (facial and object recognition tool) and ST4.4.2 (facial and object recognition tool). These DPIAs represent an initial evaluation of the data protection risks and mitigation efforts for the respective tasks. All partners have been advised to consult with organisational DPOs, some of which have already provided feedback. The DPIAs will be re-evaluated prior to the commencement of the respective tasks, as documented in the personal data processing timeline (see subsection 3.7.1 below). All LEAs intending to process real closed-case file data in the INSPECTr Living Labs have been requested to supply DPIAs for T1.3 on

[3] Open access (OA) refers to the practice of providing online access to scientific information that is free of charge to the end-user and reusable. 'Scientific' refers to all academic disciplines. In the context of research and innovation, 'scientific information' can mean peer-reviewed scientific research articles (published in scholarly journals) or research data (data underlying publications, curated data and/or raw data). See European Commission, H2020 Programme Guidelines to the Rules on Open Access to Scientific Publications and Open Access to Research Data in Horizon 2020, Version 3.2 21 March 2017.

[4] European Commission DG for Research & Innovation, *H2020 Programme Guidelines on FAIR Data Management in Horizon 2020*, 26 July 2016. http://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/oa_pilot/h2020-hi-oa-data-mgt_en.pdf

[5] Article 29 Data Protection working party Opinion WP248 Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, April 2017.

account of their unique organisational contexts. Otherwise, the LEA T1.3 DPIAs will be substantially similar as regards the processing of personal data within the INSPECTr platform. The LEAs have completed DPIAs at different timescales partly because of the differing lengths of time taken to identify their legal basis for processing – an *a priori* requirement.

## 3.3 Incidental Findings Policy & Log

Although not a Grant Agreement requirement, the existence of an Incidental Findings Policy was identified by TRI as ethically desirable for the project. Partners PHS and TRI took on the development of the policy in March 2020. Draft versions were shared with partners and the EAB for comment and in October 2020 the final version was placed on the OnlyOffice platform within the Ethics folder (see Figure 1); this is provided in Annex 1 to the present document. The Policy sets out a clear process for project decision-making should an incidental finding arise. An Incidental Findings 'Log' has also been developed to record Incidental Findings decisions within the same folder. At the time of writing, there have been no incidental findings logged.

Incidental Findings are a standing item in the WP8 monthly meetings.

## 3.4 Non-EU Transfer of Personal Data Log

The project keeps a 'Log' of project transfers of personal data from EU to non-EU countries and international organisations, as well as from non-EU countries to the EU (or another third state). Ethics requirement No. 6 in deliverable D9.4 covering this protection of personal data issue was identified as open for monitoring and the log has been established in part to ensure that partners keep track of personal data transfers. At the time of writing, two types of international data transfers have been logged: EU-UK international data transfers following the expiration of Brexit transition agreements; international data transfers to the US for an initial use of a mailing list service provider.

The International Transfer of Personal Data Log is a standing item in the WP8 monthly meetings. More details of the above-mentioned international data transfers are provided in Section 4.3 as a record of work by the Ethics Manager to ensure lawful transfers of personal data.

## 3.5 ILS INSPECTr Risk Assessment Tool

Partner ILS manages the INSPECTr risk assessment tool under task ST7.1.2. The risk assessment tool uses a standard methodology, attributing separate scores (between 1-10) to risks under 'impact' and under 'likelihood', adding the two scores together to rank the overall risk out of 20. The tool has a specific category for 'Ethics' risks. A number of ethics categorised risks have been identified by the TRI Ethics Manager and other partners within the early stages of the project. Many of these have since been removed or deescalated following mitigating measures during the first and second EC ethics check processes (June and September 2020).

The risk assessment tool is a standing item at the monthly consortium meetings.

## 3.6 Legal Basis for Processing Personal Data

Within the OnlyOffice Ethics folder, there is a sub folder entitled 'Legal Basis'. That folder keeps a record of the LEA legal basis provided by the four LEAs processing closed case file data in the Living Labs. The same folder includes copies of Legitimate Interests Assessments (LIAs) from partner CCI for activities where this forms the legal basis. It is further expected that a record of any informed consent forms will also be stored in this folder for human research activities that rely on consent.

Finally, section 6 of the INSPECTr Privacy Statement on the INSPECTr website https://inspectr-project.eu/privacy.html#research_data sets out in a transparent manner the legal basis used by partners for the processing of personal data within the project.

## 3.7 TRI 'Touchpoint Table' for Ethical Issues

Following the second EC ethics check which completed in September 2020, TRI developed and populated a tool known as the 'TRI TouchPoint Table' to track ethics issues and commitments made in the project. This tool has been used to consolidate the various commitments made in the WP9 ethics requirements deliverables. It highlights the core ethics issues identified during the project, and those most relevant for ongoing monitoring within the project. These concern the tasks which: (i) incorporate online or publicly available sources of personal data; (ii) involve personal data transfers from EU to non-EU countries and vice versa; (iii) involve AI models; and (iv) include human research participants. These areas can be observed in the blue coloured cells in Figure 3 below. The 'TRI TouchPoint Table' is also forward looking and seeks to identify ethics issues beyond the scope of the project, but which the project should consider in the design requirements. These issues are largely similar to those relevant to the project itself, with human research participation removed but with the added concern of profiling and surveillance. These areas can be observed in the grey coloured cells in Figure 3 below. If the ethics issues identified are relevant to a specific task, a tick (i.e. '√') is placed in the relevant cell, accompanied by a fuller explanation as well as the activities to which partners have committed to mitigate these risks (see, 'Explanation' and 'Addressing these issues' cells respectively).

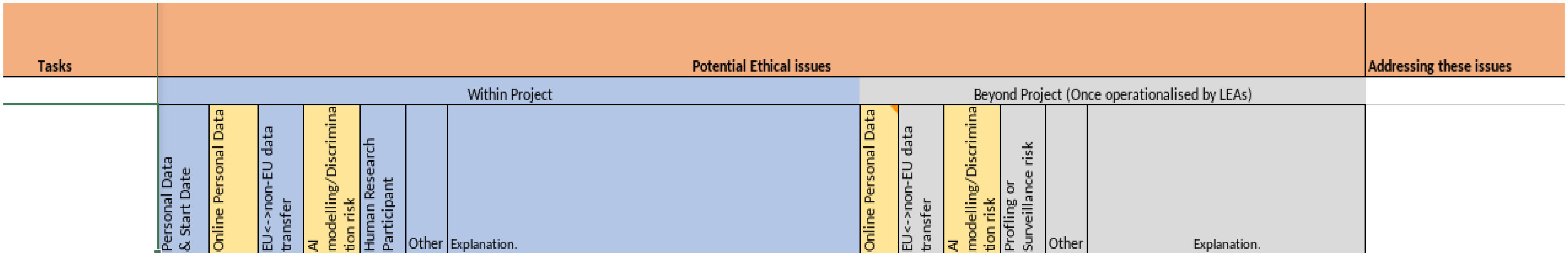
The 'TRI TouchPoint Table' has been used since November 2020 as the main ethics monitoring document for discussion of ethics issues with WP leaders during WP8 monthly meetings, and with the EAB during quarterly meetings.

### 3.7.1 Personal Data Processing Timeline

Although the project has processed only a limited amount of personal data so far, awareness between partners of the intended timeline for personal data processing is essential to ensuring that any contingent ethical commitments have been fulfilled in advance of processing. The timeline has taken various forms but since October 2020 has formed a composite part of the TRI 'TouchPoint Table' for Ethical Issues (see Figure 3 below).

The timeline is discussed with WP leads at the WP8 monthly meetings.

Figure 3: Screenshot of Headings Used in INSPECTr's 'TRI TouchPoint Table'



| Tasks | Potential Ethical issues | | | | | | | | | | | | | Addressing these issues |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Within Project | | | | | | | Beyond Project (Once operationalised by LEAs) | | | | | | |
| | Personal Data & Start Date | Online Personal Data | EU<->non-EU data transfer | AI modelling/Discrimination risk | Human Research Participant | Other | Explanation. | Online Personal Data | EU<->non-EU data transfer | AI modelling/Discrimination risk | Profiling or Surveillance risk | Other | Explanation. | |

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Grant Agreement No 833276.

# 4 Ethical Issues Experienced during M18-M24 of the INSPECTr Project

## 4.1 Application to use human participants submitted to UCD Ethics Committee

In February 2021, the project partners submitted an application to the institutional research ethics committee of the project coordinator, UCD. This submission was for the following activities:

- Surveys/questionnaires for feedback on initial platform specifications, demonstrations and testing of mocked use cases by non-consortium LEAs in workshop webinars (CCI)
- Surveys/questionnaires for feedback on Impact Assessment for LEA consortium members (ILS)
- Surveys/questionnaires (in class) to elicit feedback from LEA consortium members on pilot of training course developed to support the INSPECTr platform (UNIL)

Key individuals from the partners intending to engage in the above research activities discussed with the Ethics Manager how best to approach the submission, what research ethics topics needed to be included and considered, and how ethical issues could best be managed.

Particular attention was paid to the research subjects, and ensuring that they would not be any worse off as a result of participating in a research activity for the project. The relevance of potential physical, psychological, economic, social, legal, or environmental harms were considered and the following key areas were discussed in more detail:

1. The health and safety of participants. Due to the nature of the project, and use-cases, there are detailed descriptions of fictitious criminal investigations about criminal behaviours covering topics such as child sexual abuse, terrorism, and fraud. There will be no exposure to actual illicit material. However, touching on these topics could trigger memories of situations that might be uncomfortable or, potentially damaging. Participants are assured at every stage that they can withdraw from the activity, or leave sections unanswered if they do not wish to engage with it. If, however, participants did experience difficulties, then they are advised to seek help and are provided with a number of resources to support them. In terms of physical health, participants are asked to only participate using equipment they are familiar with, and the software was designed to be intuitive so avoid any misunderstandings that could affect the participants.
2. Selection of participants. As the project is targeting project partners and LEA officers as research participants, there is a risk that power relationships or peer-influence could create pressure for people to participate. Participants having permission to participate from an employer or manager was important as an individual's participation might coincide with their working hours, there might be a large number of respondents already from a particular organisation, or an organisation might not want a particular employee to answer. To protect research subjects, this needed to be balanced against any potential negative impacts that could be created for research subjects from their participation, or their responses. Thus, organisational permission to participate is obtained separately so that employees know they can participate if they wish, the consent form makes clear that research subjects should only participate if they choose to, no contact details of participants are shared along with the results of the activities, and any collected data is edited so that respondents cannot be identified from their answers. Further, there is no inducement or incentive for participants to engage in the activities, other than being willing to participate to benefit the research activity.

3. Informed consent. To ensure that research subjects were fully informed about the activity they were being asked to participate in before giving their consent to participate. Research subjects were given clear information sheets and informed consent forms that explained what the activity involved, what they would be consenting to, how that consent would be managed, what their rights would be as data-subjects under the GDPR, and how their responses would be used in research.
4. Privacy and data protection. As many of the participants are expected to be LEA officers, it was important to consider how personal data would be managed due to the sensitivities of their role, and the risks of operational data leakage, and how research subjects would be protected if they provided negative comments. Project partners wanted research subjects to be able to provide responses in a secure environment where their responses would not be able to be used to identify them in case they wish to be critical of the project, or their own organisation. This would require complete anonymity. However, providing anonymity to research subjects would also strip them of their rights to their personal data as data subjects. Therefore, it was decided that the responses would be pseudonymised to the effect that the partners involved in administering the survey would be able to identify a research subject if this was required, through the use of separate files containing details of research subjects in one file and their responses in another and linking them via tokens. But, research subjects would not be identifiable to others who do not have access to the required additional information. As the pseudonymised data is still personal data, this provided the functional de-identification desired to protect research subjects, whilst also retaining their ability to exercise their rights as data subjects.

Further, to ensure diversity in respondents, partners involved in recruitment are asked to purposely disseminate invites to participate to groups that represent under-represented groups, such as BAME, LGBTQ+, and women's groups.

The submission to the UCD Ethics Committee was successful, after some requested minor clarifications were provided. The response from the Committee will be provided to the EC in D9.3.

## 4.2 Processor-Controller Agreement template for LEA use of Living Labs

The success of the Living Labs (LLs) in T1.3 are a key part of the INSPECTr project. It is important for LEAs to be able to bring closed case file data into this secure environment and engage in testing of the INSPECTr tools so that the results provided are as realistic as possible. This will allow for the outputs to be a better representation of a real investigation than using mock data, and provide the technical partners with a better understanding of how the tools work and could be improved.

So that real closed case file data can be used according to LEA policies and national legislation in the LLs, it is important that the LEAs are in control of this data. Thus, from a data protection perspective, it is important that the LEAs are Data Controllers.[6] However, from a technical perspective, it was important to recognise that the LEAs are not as familiar with the INSPECTr tools that are under development as the technical partners. Therefore, technical partners (CCI and PHS) would need some access to the LLs in case technical assistance needed to be provided to the LEAs. This access would involve an INSPECTr tool that is not working as it should be being transferred from an LEA INSPECTr node to a development node where technical partners could provide assistance. No technical partners would have access to an LEA node, but LEA closed case file data might be

[6] Art.4(7), European Parliament and Council, Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, OJ L 119, Vol.59, 4 May 2016 (General Data Protection Regulation, hereafter: GDPR)

captured by the tool when in the LEA node and, if technical assistance is needed, such data would then be transferred to the development node.

Due to the very wide definition of 'processing' under the GDPR covering '*any operation … which is performed on personal data*',[7] it is likely that in rendering technical assistance to LEAs in a LL, that technical partners would engage in 'processing'. Consequently, it is important that the data processing relationship between LEAs and technical partners for the processing of closed case file data is adequately determined.

A Joint Controllership scenario, where both LEAs and technical partners would decide on the purposes and means or processing[8] (how's and why's) was considered. However, this would put the LEAs in a difficult position as they need to maintain control over closed case file data which, by its nature, is highly sensitive. Therefore, a Controller-Processor relationship[9] is thought to be most appropriate as this will provide LEAs with control over their data. Technical assistance will be provided by technical partners at the LEA's discretion.

However, as engaging in a research project with such a high-level of technical complexity as INSPECTr has not been a common experience for most of the LEAs, it was decided that the Ethics Manager should draft a template Controller-Processor contract for the LEAs to adapt to their needs. This would also provide consistency across the multiple Controller-Processor relationships between multiple LEAs and the same technical partners. However, due to the particular legal arrangement of AGS, they decided to develop their own Controller-Processor contract. The Ethics Manager discussed contract contents with AGS to ensure that there was still a level of consistency.

Following completion of DPIAs by the LEAs involved in the LLs, the Controller-Processor contract template is shared, the particular needs of each LEA are taken into account during meetings between the LEAs and the Ethics Manager, and then contracts are submitted to LEA legal teams/DPOs for review and consultation. Where necessary, such contracts will also be provided to national data protection authorities during consultations with those organisations too.

## 4.3 International Data Transfers

### 4.3.1 Transfers of Personal Data to UK-based partners

As noted above, following Brexit, the UK and EU agreed in their Trade and Cooperation Agreement that the UK should not be treated as a Third Country for the purposes of international data transfers for 6 months.[10] However, during the project, this time limit ran out. Happily, the EU has deemed the UK's data protection regime as providing an 'adequate' level of protection for EU data subjects,[11] meaning that international data transfers between EU and UK-based partners can continue under Art.45, GDPR. However, during discussions with the Ethics Advisory and Review Group, it was recognised that there is a potentially significant chance that either the UK will attempt to alter its data protection regime, in which case the Adequacy Decision will no longer apply if

[7] Art.4(2), GDPR

[8] Art.26, GDPR

[9] See Arts.4(7) and (8), 24, and 28, GDPR

[10] Article FINPROV.10A(4), Trade and Cooperation Agreement between The European Union and The European Atomic Energy Community, of the one part, and The United Kingdom of Great Britain and Northern Ireland, of the other part, 31.12.2020, OJ L 444/14. See, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2020.444.01.0014.01.ENG

[11] Commission Implementing Decision of 28.6.2021 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom, Brussels, 28.6.2021 C(2021) 4800

such changes result in a less than adequate level of data protection,[12] or it will be subject to legal challenge owing to the legal regime around access to data by UK intelligence agencies and so be struck down by a court.[13] As such, the Ethics Manager has been exploring back-up options.

Transfer Adequacy Assessments have been conducted by the Ethics Manager and UK-based partners, and have been discussed with the UCD legal team. The most reliable back-up option would seem to be Standard Contractual Clauses on a Controller-Controller basis, which would provide for continuing international data transfers under Art.46, GDPR between EU and UK-based partners in the project. The Ethics Manager drafted a document including such clauses, which was signed by TRI. However, the other UK-based partner, PSNI, is considering if it would be appropriate for their organisation to sign the document as the clauses require an organisation to be liable for harms caused to data subjects. The Ethics Manager is exploring alternative arrangements which will be discussed with the Ethics Advisory and Review Group.

It is important to note also that the Standard Contractual Clauses made available by the EC have also been revised. The Ethics Manager will soon re-draft the Standard Contractual Clauses on a Controller-Controller basis and implement them.

It should also be noted that the UK implemented the GDPR in its national law under the Data Protection Act 2018. Since Brexit, it has also copied the GDPR into UK law as the ‘UK GDPR’. The UK’s Information Commissioner has made an ‘Adequacy Regulation’ with respect to the transfer and protection of personal data transferred from the UK to the EU.

### 4.3.2 Transfers of Personal Data to the US

As part of the project’s dissemination effort, it is important to be able to provide a newsletter to potentially interested parties. Due to the large size of mailing lists for projects like INSPECTr, it is often useful to use a mailing list service to administer the mailing list. Initially, a US-based mailing list provider was used. However, following the *Schrems II* judgement,[14] it was decided to switch to an EU-based mailing list provider.

This was an important step as, following the *Schrems II* judgement, the main mechanism for lawful international data transfers to the US (Privacy Shield) was struck down in this case. This is due to the extent of the potential access for US intelligence agencies into the personal data of EU data subject when held on US-based servers. Whilst Standard Contractual Clauses have been implemented by some US-based companies, including the mailing list service provider use by the project, their lawful use is questionable[15] as the personal data of EU data subjects would still be accessible to US intelligence agencies and the amount of technical safeguards that would need to be implemented (e.g. strong encryption) would render the data useless once in the US. As such, the Ethics Manager recommended switching to an EU-based mailing list service provider, and this move has now been completed.

[12] Article 3, Commission Implementing Decision of 28.6.2021 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom, Brussels, 28.6.2021 C(2021) 4800

[13] Osal Stephen Kelly, ‘The UK Adequacy Decision and the Looming Possibility of a Schrems III’, KSLR EU Law Blog, 10.05.2021. Available at: https://blogs.kcl.ac.uk/kslreuropeanlawblog/?p=1549

[14] Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems, Case C-311/18 (Schrems II)

[15] Irish Data Protection Commission, ‘DPC statement on CJEU decision., Press Releases, 16.07.2020. Available at: https://www.dataprotection.ie/en/news-media/press-releases/dpc-statement-cjeu-decision

## 4.4 The potential impact of the EU's proposed AI regulation

Following several years of discussions about ethical and trustworthy AI systems at EU level, in April 2021 the European Commission provided a proposal for a Regulation for AI systems.[16] This proposal is currently at consultation stage, to be followed by likely lengthy negotiations. As the INSPECTr project is currently due to finish in February 2023, the Ethics Manager considers that it would be unlikely for such a major piece of EU-level legislation to have legal effect before the end of the project.[17] Therefore, whilst it is expected that no legal obligations will affect the INSPECTr partners, or the tools they create, during the project, obligations regarding those tools involving AI are likely to apply in the years following the project, when the tools are likely to still be in use.

Following the current proposed draft, the INSPECTr tools are unlikely to be prohibited. One type of prohibited AI system are those for real-time biometric identification.[18] The INSPECTr project is developing facial recognition tools, but they are not expected to be used in real-time. If these tools are adapted for real-time use by LEAs, then there is an exception that allows for the use of such systems for law enforcement purposes.[19] As such, the INSPECTr tools are likely to be classed as 'high-risk'. This is due to the use of biometric identification and categorisation tools,[20] and, primarily, because of use by LEAs.[21] This means that the proposed AI Regulation as it currently stands would apply to the INSPECTr tools.

However, bearing in mind the likely regulatory time-line, there is no critical legal obligation for the project to comply with the proposed AI regulation. Still, the Ethics Manager is reviewing potential impacts to try and 'future-proof' the INSPECTr tools ahead of them being used so that end-users will face limited barriers to using the tools once the Regulation is in-force.

Fortunately, several aspects of the proposed AI Regulation already include topics that the WP8 team is planning on working on. This includes transparency, bias, oversight, and logging. The Ethics Manager will adapt planned work to take account of the proposed AI Regulation, bearing in mind that it will likely change before adoption.

## 4.5 Anonymisation of real case data, and of real mobile phone data

### 4.5.1 Exploring the use of real and realistic data by Consiglio Nazionale Delle Richerche

For CNRs work on data parsers, it is ideal, from a technical perspective, to use real closed case, or at least realistic, data in order to adequately test the ability of this tool to connect data together. CNR are mindful of the need for data to be processed in compliance with the applicable data protection legislation, and in respect of privacy concerns, which are highly pertinent to the use of real closed case data.

During work on data parsing, CNR first considered the potential of anonymising a real closed case which they could access. This plan was discussed at a WP8 monthly meeting. The technical benefit of the data to the project

[16] Proposal for a Regulation of the European Parliament and of the Council laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and amending Certain Union Legislative Acts COM/2021/206 final, 21.04.2021 (hereafter: Proposed AI Regulation). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1623335154975&uri=CELEX%3A52021PC0206

[17] For comparison, the GDPR was first proposed in 2011, was agreed in 2016, and came into force in 2018.

[18] Art.5(1)(d), Proposed AI Regulation.

[19] Art.5(1)(d)(iii), (2), (3), and (4), Proposed AI Regulation.

[20] Para.(1), Annex III, Proposed AI Regulation.

[21] Para.(6), Annex III, Proposed AI Regulation.

was acknowledged. The Ethics Manager and other attendees discussed where the data would come from, and how it could be anonymised. There was agreement that due to the nature of the data, it might be possible for it to be anonymised. However, in order for the data to be anonymised, this would require some (pre-)processing.

As the closed case file included personal data and, due to the nature of the data, special category data, as well as the data in the file being related to criminal offences/convictions. Consequently, this would require a legal basis for the processing of personal data under Article 6, GDPR, an exemption that would allow for the processing of special category data under Article 9(2), GDPR, and an exemption under Article 10 that would allow for the processing of personal data related to criminal offences/convictions.[22] Following internal discussion, CNR opted to not pursue the processing of this dataset before any legal basis information was determined.

Instead of anonymising real closed case file data, CNR began looking at realistic data that did not come from a criminal case. The proposed data would be anonymous metadata extracted from a mobile phone, where the data was extracted and anonymised outside of the INSPECTr project in another activity. Due to being anonymous data, this minimised data protection issues. With respect to privacy issues from an ethical perspective, the Ethics Manager explained that it would be best for all persons whose data was originally processed to create the anonymous metadata were aware of this activity, to which CNR agreed.

### 4.5.2 Anonymising datasets by Gendarmerie Nationale

Due to the organisational requirements of GN, they are not in a position to process personal data within the INSPECTr project. Thus, for any datasets they consider using, a determination must be made on whether the dataset contains personal data and whether it could be successfully anonymised.

Personal data has four elements: (1) ’any information’ (2) ‘relating to’ (3) ‘an identified, or identifiable’ (4) ‘a natural person.’[23] The third element here is crucial. Under the GDPR, data can only be considered to be anonymised where it is no longer ‘*reasonably likely*’ that a person can be identified, considering all objective measures.[24] This is a high-bar to reach as consideration should be given not just to the actions of individuals who are expected to use the data, including any contractual obligations not to attempt re-identification, but also potential attackers/hackers who might be able to acquire data and re-identify data subject. Further, there is a ‘release and forget’ issue that must be considered; data that is considered to be anonymous has been openly released in the past, only for new technical techniques and processes to be used to re-identify the data subjects.[25] Thus, whilst data might be considered anonymous now, it might not be anonymous in a few years.

Bearing these factors in mind, the Ethics Manager has discussed several potential datasets with GN staff in terms of their potential to be anonymised and used in the project. For the suggested datasets, it was agreed that anonymisation would not be possible and so GN should not make use of the proposed datasets. The potential ability of GN to anonymise datasets is a continuing discussion with the Ethics Manager whenever new datasets are suggested.

[22] Article 10, GDPR allows for the processing of personal data related to criminal offences/convictions on the basis of an official authority. Although CNR are a public organization, it is not thought that they have an official authority to process such data.

[23] See Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, 01248/07/EN, WP 136, Adopted on 20th June 2007.

[24] Recital 26, GDPR.

[25] Mark Elliot, Elaine Mackey, and Kieron O’Hara, ‘The Anonymisation Decision-Making Framework: European Practitioner’s Guide’, UK Anonymisation Network, 2020. p.14

## 4.6 Ethics and Privacy-by-design

Ethics and Privacy-by-design is a key part of ethics governance in INSPECTr. It is a continuous process of discussing proposed activities to consider ethics and privacy issues. These discussions occur at all meetings that the Ethics Manager attends, as discussed in Section 2 above. These can range from short discussions where the Ethics Manager highlights ethical issues that might be relevant to, and should be considered, as part of deliberating on technical points, up to in-depth research and reporting by the Ethics Manager on particular issues. This is done to embed ethics and privacy considerations into the development of the INSPECTr tools and platform. However, the substantive discussion on issues that have been discussed as part of the Ethics and Privacy-by-Design process are discussed in D8.7 (M24).

# 5 Conclusions

This deliverable is the second INSPECTr report on ethical governance and has set out the ethical management processes, tools, and issues encountered between months 18 and 24 of the project.

Sections 2 and 3 have been updated to cover the ethics governance process in INSPECTr, and the monitoring tools that are used.

Section 4 contains new information about the topics that have been considered and discussed as part of the ethics governance process between months 18 and 24.

# 6 Annex 1: INSPECTr Incidental Findings Policy

## Intelligence Network & Secure Platform for Evidence Correlation and Transfer

## Incidental Findings Policy

### Document Summary Information

| | |
|---|---|
| **Responsible Author** | Yves Vandermeer (PHS), Leanne Cochrane (TRI) |
| **Contributions from** | Joshua Hughes (TRI) |

***Revision history (including peer reviewing & quality control)***

| Version | Issue Date | % Complete | Changes | Contributor(s) |
|---|---|---|---|---|
| v0.1 | | 0 | Initial Structure | Yves Vandermeer |
| V0.2 | | | Review and Project Process Added | Leanne Cochrane |
| V0.3 | 29.09.20 | | Review and Comment on Section 1.2.1 concerning criminal activity still being an IF since not project objective. | Yves Vandermeer |
| V0.4 | 01.10.20 | | Amend to section 1.2.1 to reflect YV comment. | Leanne Cochrane |
| V0.5 | 20.10.20 | | Amend to page 7 giving specific TULSA example following Ethics Board review and comment. | Yves Vandermeer/Leanne Cochrane |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

***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***

# Table of Contents

1 Introduction ........ 28
1.1 What are Incidental Findings ........ 28
1.2 Incidental Findings within the INSPECTr Project ........ 28
1.2.1 Distinguishing Incidental Findings and the Intended Objective of the Living Lab Use Cases ........ 29
2 The INSPECTr Reporting Process ........ 30
2.1 Directions on How the Project Should Handle Different Types of Incidental Findings ........ 30
2.1.1 Criminal Activity ........ 30
2.1.2 Other non-criminal findings ........ 31

# List of Figures

Figure 1: INSPECTr Reporting Process for Suspected Incidental Findings ........ 32

# Glossary of terms and abbreviations used

| Abbreviation / Term | Description |
|---|---|
| LEA | Law Enforcement Agency |
| IF | Incidental Finding |
| IMEI | International Mobile Equipment Identity |
| | |
| | |
| | |

# 1 Introduction

This Incidental Findings Policy is intended to provide researchers (technical, LEA and other partners) with guidance on what to do with unexpected project findings. This Policy is intended to supplement, not replace, pre-existing obligations. It is important that the various types of incidental findings are dealt with appropriately, to minimise the risk to individuals.

The first step in addressing incidental findings is to endeavour to mitigate such findings before they occur. The principle of data minimisation is important in this regard. Partners do however recognise that it is not possible to fully eradicate the risk of all incidental findings. That means that scenarios not anticipated by this document could also arise. As such, this Policy is intended to outline a general guide and should not be considered exhaustive.

## 1.1 What are Incidental Findings

Incidental finds are results which are outside the scope of the research.[26] These results are often referred to as 'unintended', 'unexpected' or 'incidental'. According to the EC, a characteristic of incidental/unexpected findings is that they require the researcher to take some form of action.[27]

The concept of incidental findings arises most commonly in medical research, where for example, the testing of a new medical technology might reveal information about the genetic susceptibility that someone might have to a serious disease; this creates an issue about whether researchers should inform the participants.[28]

Incidental findings may include indications of criminal activity, such as human trafficking, abuse, domestic violence or bullying,[29] but can also include other types of unexpected results such as revealing sensitive personal data, or sensitive organisational information, e.g. suicide risks or misconduct.

## 1.2 Incidental Findings within the INSPECTr Project

Within the INSPECTr project, the possibility of uncovering incidental findings pertaining to criminality could occur from both the activities of technical partners and LEAs where real data is being used.

- *Example: Child abuse materials found on a dataset where a different crime is expected, e.g. fraud, stalking, corruption (or vice versa);*
- *Example: Phishing email found on a dataset;*
- *Example: Online platform post where an individual boasts about criminal activity;*
- *Example: New evidence in closed cased files.*

[26] https://ec.europa.eu/research/participants/data/ref/h2020/other/hi/h2020_ethics-soc-science-humanities_en.pdf, p14.

[27] Ibid. p.14

[28] See generally on this area, European Commission, *European Textbook on Ethics in Research*, Director-General for Research, Science, Economy and Society, Brussels, 2010, p.192.

[29] https://ec.europa.eu/research/participants/data/ref/h2020/other/hi/h2020_ethics-soc-science-humanities_en.pdf, p14.

It is also possible that researchers within the INSPECTr project might unintentionally find 'personal data' that was not intended to be collected and not related to any crime, such as medical information or information about an individual's personal life which could be compromising. Within INSPECTr, some examples might include:

- *Example: the IMEI of the personal mobile phone of the person who contributed to the creation of a mocked dataset for a use case is discovered and reported by the system;*
- *Example: the name, e-mail address and date of birth of a software developer is recovered from a strings extraction and reported by the system.*

### 1.2.1 Distinguishing Incidental Findings and the Intended Objective of the Living Lab Use Cases

It is important to be clear that because INSPECTr is a project focused on developing an intelligence sharing network for LEAs as well as digital forensics tools, the project intends **in advanced stages** to test the INSPECTr platform on real investigation case files within the INSPECTr Living Labs.

In this case, LEA partners will be deploying much of the INSPECTr platform (See T1.3) in the same way they would intend to use the tools during criminal investigations.

A number of safeguards are however in place to ensure that the project **maintains the objective of building a successful platform, rather than uncovering new criminal activity**. These are as follows:

- **Only closed case file data in Living Labs** – Using closed case files in the Living Labs reduces the risk of the project uncovering new criminal activity. (It has the added advantage of allowing the project to compare the success of the analysis of the INSPECTr platform against the original case file, e.g. pattern identification, relevant digital forensic material etc.)
- **No web scraper testing by LEAs in Living Labs** – Only the technical developer will test the web scraper on a limited amount of real online data in the latter stages of the scraper's development. By not including the web scraper in the Living Labs for LEA testing, the risk of LEAs identifying ongoing criminal activity is reduced.

Despite INSPECTr's efforts to reduce the risk of uncovering incidental (criminal) findings during the project, the risk remains moderate because of the nature of the tool being developed.

Where data is uncovered by the Living Lab testing process which suggests ongoing criminal activity, such data will be considered an incidental finding and should be dealt with in accordance with the procedures outlined below.

# 2 The INSPECTr Reporting Process

**INSPECTr Partners must report suspected incidental findings to the INSPECTr Project Coordinator (with Project Manager in cc) along with any organisational actions taken.**

**This information should also be recorded by the Partner in the Incidental Findings Log (OnlyOffice - 'Ethics' folder).**

The Project Coordinator will constitute a project 'Incidental Findings Review Team' to determine how to handle the findings. The Review Team will include:

| **Role** | **Person** |
|---|---|
| **Project Coordinator, CCI**<br>**Project Manager** | Cheryl Baker, or other CCI designee<br>Vivienne Kearns, or other CCI designee |
| **LEA Representative** | Yves Vandermeer, or other LEA designee |
| **Ethics Manager** | Joshua Hughes, or other TRI designee |
| **Ethics Board member** | Daragh O Brien/ Katherine O'Keefe, or other EB designee |
| **Partner who uncovered incidental finding** | *Case by case basis* |

The Project Review team's assessment and determination on Incidental Findings should co-exist alongside any Partner's established organisational process which they should also follow. The relevant partner is responsible for ensuring that the INSPECTr project coordinator is updated on any separate organisational actions.

The Ethics Manager is responsible for keeping a record of the decision of the Project Review Team. This should be recorded in the Incidental Findings Log.

## 2.1 Directions on How the Project Should Handle Different Types of Incidental Findings

The following directive factors should be considered by the INSPECTr Project Incidental Findings Review Team when assessing and determining on incidental findings.

### 2.1.1 Criminal Activity

According to the EC Guidance on 'Ethics in Social Sciences and Humanities', the default position is that criminal activity should be reported to the responsible and appropriate authorities:

> *As a rule,* ***criminal activity witnessed or uncovered in the course of research must be reported to the responsible and appropriate authorities,*** *even if this means overriding commitments to participants to*

> *maintain confidentiality and anonymity. There may be a legal obligation to report criminal activity. In some research settings (for example when working with refugees), it may be more appropriate to contact relevant NGOs or agencies with appropriate expertise rather than the authorities.*[30]

All INSPECTr partners should adhere to domestic law which requires that the responsible and appropriate authorities are informed about suspected criminal activity.

If the criminal activity is considered time-critical (e.g. where a person is at immediate risk of harm), this should be the first priority.  As with all incidental findings, it should additionally be reported to the Project Coordinator, who will refer the matter to the Incidental Findings Project Review Team, as well as your organisation's Data Protection Officer and Legal Team, where applicable.

The INSPECTr Project recognises that the partners experience different legal obligations and responsibilities, typically of a heightened nature if the partner is publicly funded and/or operates under a statutory mandate. Similarly, a minority of countries place their private citizens under obligations to report crimes. This is particularly relevant to INSPECTr partners who are LEAs. As public authorities, they may be legally obligated to investigate crimes which are reported to them. For example, European human rights law requires LEAs to investigate where threats to life are made.[31] Again, if LEAs in the course of their participation in research activities for INSPECTr discover information or evidence relating to criminal activity, they should follow their organisational policy and legal obligations.

Beyond the organisational policy decisions of the individual partners, whether information pertaining to suspected criminal activity should be reported to LEAs or other appropriate authorities by the Project, is a decision to be taken by the INSPECTr Project Review Team. The process will apply the existing specific national legislation or regulation related to the type of crime (e.g. Terrorism, Child Abuse, Money laundering,  Chemical or Biohazard risks, ...).  For example, in Ireland, findings which indicate a potential of harm or risk to a child may require mandatory reporting to the Child and Family Agency (TUSLA) under the Children First Act 2015. While the team will work from the default position of reporting suspected criminal activity, each finding will be assessed on a case by case basis and depend on the specific nature of the information found.

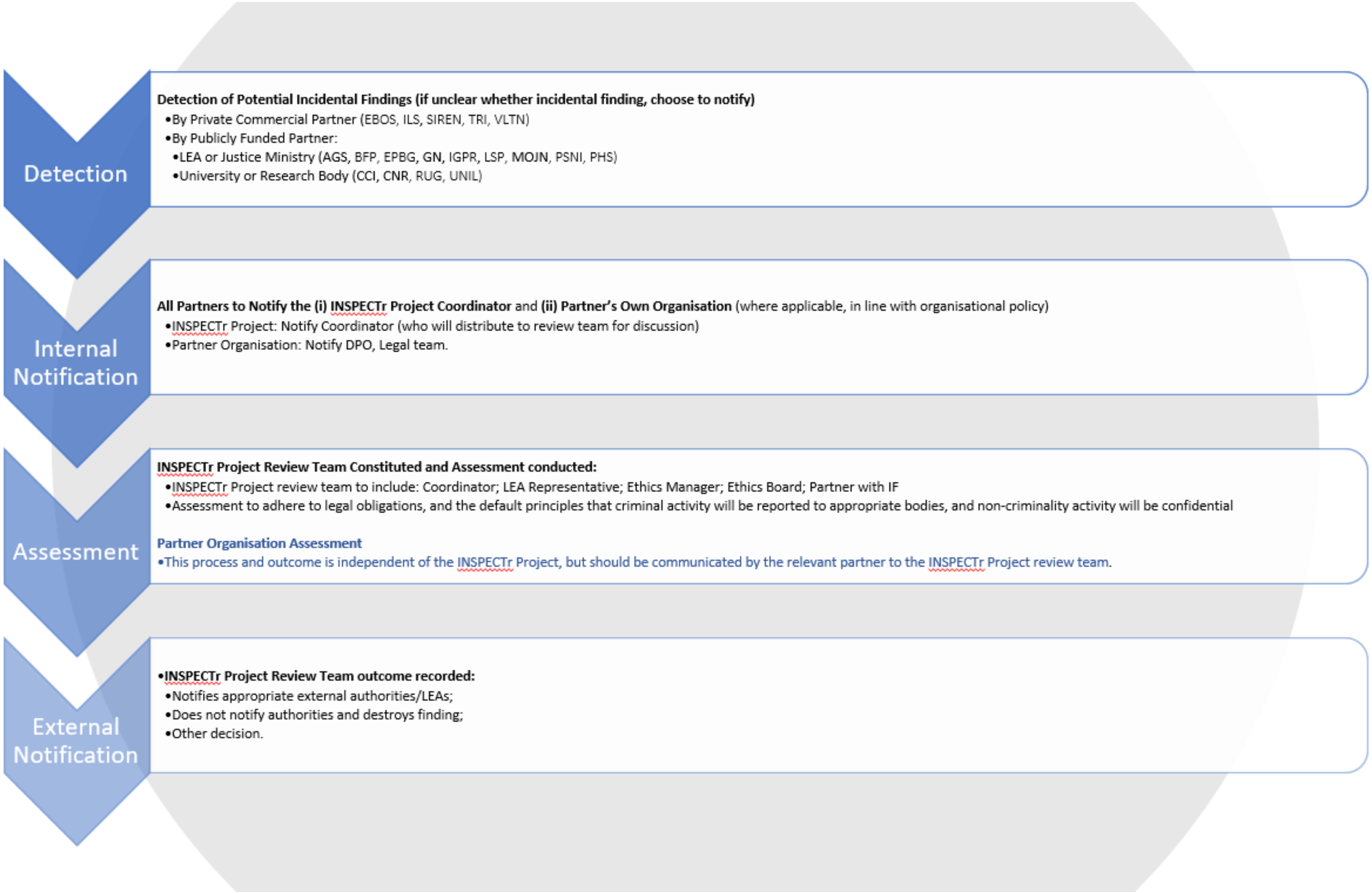
### 2.1.2 Other non-criminal findings

Where an incidental finding does not involve suspected criminal activity, the project should be guided by the importance of the ***principle of confidentiality*** in research ethics.[32] As suggested above, this principle of confidentiality may not apply where there is risk of harm, such as in a criminal context.  In other situations, it may be important to avoid civil harms to the individual; and in other cases, it may be appropriate to notify the individual or organisation at risk of harm of the finding to take mitigating or safeguarding actions.

[30] https://ec.europa.eu/research/participants/data/ref/h2020/other/hi/h2020_ethics-soc-science-humanities_en.pdf , p14.

[31] Osman v UK, Judgment (Case No. 87/1997/871/1083, 28 October 1998), paras.116.

[32] European Commission, *European Textbook on Ethics in Research*, Director-General for Research, Science, Economy and Society, Brussels, 2010, pp.79-80.



Detection

**Detection of Potential Incidental Findings (if unclear whether incidental finding, choose to notify)**

- By Private Commercial Partner (EBOS, ILS, SIREN, TRI, VLTN)
- By Publicly Funded Partner:
  - LEA or Justice Ministry (AGS, BFP, EPBG, GN, IGPR, LSP, MOJN, PSNI, PHS)
  - University or Research Body (CCI, CNR, RUG, UNIL)

Internal Notification

**All Partners to Notify the (i) INSPECTr Project Coordinator** and **(ii) Partner's Own Organisation** (where applicable, in line with organisational policy)

- INSPECTr Project: Notify Coordinator (who will distribute to review team for discussion)
- Partner Organisation: Notify DPO, Legal team.

Assessment

**INSPECTr Project Review Team Constituted and Assessment conducted:**

- INSPECTr Project review team to include: Coordinator; LEA Representative; Ethics Manager; Ethics Board; Partner with IF
- Assessment to adhere to legal obligations, and the default principles that criminal activity will be reported to appropriate bodies, and non-criminality activity will be confidential

**Partner Organisation Assessment**

- This process and outcome is independent of the INSPECTr Project, but should be communicated by the relevant partner to the INSPECTr Project review team.

External Notification

- **INSPECTr Project Review Team outcome recorded:**
  - Notifies appropriate external authorities/LEAs;
  - Does not notify authorities and destroys finding;
  - Other decision.

Figure 4: INSPECTr Reporting Process for Suspected Incidental Findings

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Grant Agreement No 833276.