EVIDENCE2 / e-CODEX

Linking EVIDENCE into e-CODEX for EIO and MLA procedures in Europe

JUSTICE PROGRAMME (2014-2020)

JUST-JCOO-CRIM-AG-2016

Action Grants to Support Transnational Projects to Promote Judicial Cooperation in Criminal Matters

Grant Agreement No. 766468

EVIDENCE2E-CODEX

Linking EVIDENCE into e-CODEX for EIO and MLA procedures in Europe

Conclusion report and feedback from the Joint WP3/WP4 Technical Workshop validating the Evidence Exchange Standard Package Application

Deliverable D4.2

This project was funded by the European Union's Justice Programme (2014-2020) under Grant Agreement No. 766468

Project co-funded by the European Commission within the Justice Programme (2014-2020)		
Dissemination Level:		
PU	Public	X
CO	Confidential, only for members of the consortium (including the Commission Services)	
EU-RES	Classified Information: RESTREINT UE (Commission Decision 2005/444/EC)	
EU-CON	Classified Information: CONFIDENTIEL UE (Commission Decision 2005/444/EC)	
EU-SEC	Classified Information: SECRET UE (Commission Decision 2005/444/EC)	

Document Version Control:		
Version 0.1	Originated by: INTERPOL	On 04/04/2019 at 17H30
Version 0.2	Originated by: INTERPOL	On 09/04/2019 at 10H02
Version 0.3	Originated by: INTERPOL	On 12/04/2019 at 16H40
Version 0.4	Reviewed by: INTERPOL	On 16/04/2019 at 17H00
Version 0.5	Reviewed by: INTERPOL	On 18/04/2019 at 10H32
Version 0.6	Reviewed by: INTERPOL	On 23/04/2019 at 14H00
Version 0.7	Reviewed by: INTERPOL	On 24/04/2019 at 16H08
Version 0.8	Reviewed by: INTERPOL	On 25/04/2019 at 16H50
Version 0.9	Reviewed by: CETIC	On 30/04/2019 at 16H00
Version 0.10	Reviewed by: K&I	On 30/04/2019 at 17H30
Version 0.11	Reviewed by: Alexandra Tsvetkova (LIBRe)	On 07/05/2019 at 11H51
Version 0.12	Reviewed by: INTERPOL	On 02/05/2019 at 10H50
Version 0.13	Reviewed by: Prosecutor General's Office, Portuguese Ministry of Justice	On 08/05/2019 at 11H45
Version 0.14	Reviewed by: LIF	On 08/05/2019 at 14H10
Version 0.15	Reviewed by: INTERPOL	On 10/05/2019 at 14H55

This project was funded by the European Union's Justice Programme (2014-2020) under Grant Agreement No. 766468

Table of Contents

Table of Contents 3
List of Abbreviations 4
Executive Summary 6
1 Introduction 8
2 Overview 10
2.1 Objective 10
2.2 Structure 12
2.3 Stakeholders 13
3 Discussions 15
3.1 Presentations 16
3.1.1 CASE overview 16
3.1.2 Data Protection and Fundamental Rights issues in the exchange of e-evidence 17
3.1.3 e-Evidence Digital Exchange system 19
3.2 Panel Sessions 20
3.2.1 Panel 1 EESP Application Functionalities & e-Evidence Digital Exchange System 21
3.2.2 Panel 2 CASE: Forensic tool companies, forensic labs and LEA perspectives 22
3.2.3 Panel 3 Legal issues, data protection and other concerns 23
3.2.4 Panel 4 Exchange of large files of evidence 26
3.2.5 Panel 5 Other platforms in use for the evidence exchange 28
4 Dissemination 32
5 Conclusion 34
6 Annexes 36
Annex 1: Agenda 37
Annex 2: List of Participants 38
Annex 3: Logistical Note 39
Annex 4: Invitation Letter 40
Appendices 41
A. Updated version of the Report on Task 4.1 “Identifying and mapping stakeholders” 41

This project was funded by the European Union’s Justice Programme (2014-2020) under Grant Agreement No. 766468

List of Abbreviations

Acronym	Explanation
AI	Artificial intelligence
CASE	Cyber-investigation Analysis Standard Expression
CJEU	Court of Justice of the European Union
CNR-ITTIG	National Research Council (Italy) - Institute of Legal Information Theory and Techniques, coordinator of the EVIDENCE2e-CODEX Project
EC	European Commission
ECtHR	European Court of Human Rights
e-CODEX	e-Justice Communication via Online Data Exchange
EESP	Evidence Exchange Standard Package
e-evidence	Electronic evidence
EIO	European Investigation Order
EJN	European Judicial Network
e-MLA	Electronic Mutual Legal Assistance
EP	Evidence Package
EU	European Union
Europol	The European Union's law enforcement agency
EUROJUST	The European Union's Judicial Cooperation Unit
EVIDENCE	'European Informatics Data Exchange Framework for Court and Evidence' Project, GA No 608185
EVIDENCE2e-CODEX	'EVIDENCE2e-CODEX Linking EVIDENCE into e-CODEX for EIO and MLA procedures in Europe' Project, GA No 766468
GA	Grant Agreement
GUI	Graphical User Interface
GDPR	General Data Protection Regulation
INTERPOL	International Criminal Police Organization
ISP	Internet Service Provider

This project was funded by the European Union's Justice Programme (2014-2020) under Grant Agreement No. 766468

JIT	Joint Investigation Team
K&I	Knowledge and Innovation Srl. (Italy), partner in the EVIDENCE2e-CODEX project
LEA	Law enforcement agency
LIBRe	LIBRe Foundation (Bulgaria), partner in the EVIDENCE2e-CODEX project
MLA	Mutual Legal Assistance
MoJ	Ministry of Justice
MS	Member States
UCO	Unified Cyber Ontology
UMF	Universal Message Format
WG	Working Group
WP	Work Package

This project was funded by the European Union's Justice Programme (2014-2020) under Grant Agreement No. 766468

Executive Summary

Deliverable D4.2 "Conclusion report and feedback from the Joint WP3/WP4 Technical Workshop validating the Evidence Exchange Standard Package Application" is drafted in conformity with the Grant Agreement of the "Linking EVIDENCE into e-CODEX for EIO and MLA procedures in Europe" (EVIDENCE2e-CODEX) project. The Joint WP3/WP4 workshop held in The Hague on 26 and 27 March 2019, was co-organised by INTERPOL (leader of WP4) together with CNR-ITTIG (project coordinator), CETIC and LIBRe (partner responsible for dissemination and communication activities). The workshop was hosted by the Dutch Ministry of Justice and Security.

The report starts with a general presentation of the event objectives, structure and participants. The joint WP3/WP4 workshop "Meeting the technical community to validate the Evidence Exchange Standard Package Application" aimed to engage the technical community with the EVIDENCE2e-CODEX achievements and goals, by informing technicians that serve the legal community about available instruments and back office needs for enabling evidence exchange via e-CODEX. The report details the event structure facilitating the attainment of set objectives. The deliverable describes the background of event attendees as a key element in fulfilling the project aim to engage relevant stakeholders. The report continues with an outline of the workshop's content, covering the essence of the discussions held during the panel sessions preceded by thorough explanations of the EESP tool, its functionalities, uses and scenarios. The event provided the opportunity to demonstrate the EESP application and to discuss its content in detail with technical experts in the area, representing both prospective end-users of the tool, as well as digital forensic tool developers. The deliverable mentions the dissemination efforts undertaken prior to, during and following the event.

The report ends with conclusions and observations shared by the stakeholder community regarding the EESP tool and the broader EVIDENCE2e-CODEX goals. The workshop participants were unanimous about the potential benefit of the EESP in facilitating the transnational exchange of evidence packages by enabling authorities to work with a standardised validation tool. The choice of the CASE standard was supported and it was agreed that the tool should integrate all of

This project was funded by the European Union's Justice Programme (2014-2020) under Grant Agreement No. 766468

the MS evidence admissibility requirements in order to present a strong and viable solution. The experts highlighted the importance of a user-friendly EESP application to ensure its uptake as a voluntary instrument by end-users.

The consortium collected and analysed the expert feedback for integration into the project's future development. This valuable input and suggestions for improving the application contribute to ensuring that the developed EESP tool offers a feasible solution that is compliant with stakeholder needs and requirements. The feedback was also incorporated into deliverable D3.3 "Final workshop with digital forensic and legal experts on the formal language for the evidence exchange representation". A final WP4 workshop will be held in September 2019 bringing together technical and legal communities to cross-fertilize their views on challenges and issues identified within the EVIDENCE2e-CODEX project.

This project was funded by the European Union's Justice Programme (2014-2020) under Grant Agreement No. 766468

1 Introduction

The present document constitutes deliverable D4.2 "Conclusion report and feedback from the joint WP3/WP4 Technical Workshop dedicated to validating the Evidence Exchange Standard Package Application" of 'EVIDENCE2e-CODEX linking EVIDENCE into e-CODEX for EIO and MLA procedures in Europe' project (EVIDENCE2e-CODEX). EVIDENCE2e-CODEX is a European Union funded project under the Justice Programme (2014-2020) that seeks to create a legally valid instrument for the exchange of digital evidence over the e-Justice Communication via Online Data Exchange (e-CODEX) platform in the framework of Mutual Legal Assistance (MLA) and European Investigative Order (EIO) procedures.

Deliverable D4.2 "Conclusion report and feedback from the joint WP3/WP4 Technical Workshop validating the Evidence Exchange Standard Package Application" is prepared within the scope of WP4 "Stakeholder engagement, Mutual learning and Capacity Building for Professionals, Policy makers and Technicians" efforts. To contextualise the event, below is an extract of the WP4 objectives and activities as listed in the Grant Agreement (GA):

Objectives

Providing stakeholders with 'ready for use' information on EIO, electronic evidence and e-CODEX. The European Judicial Training Network (EJTN) organizes workshops on the topic of electronic evidence and EIO, and therefore it will be a natural partner to share and distribute details about the workshops. For the future we foresee a closer working relationship with EJTN.

Description of work and role of partners

WP4 - Stakeholder engagement, Mutual learning and Capacity Building for professionals, Policy makers and technicians [Months: 1-21]
CNR, RUG, CETIC, ELF, LIF, INTERPOL, K&I , MoJ-NL, MoJ-DE, MoJ-IT, LIBRe, BMJ-AT, MoJ-FR, MoJ-PT, UNI-THESS, UOM, UNIL-CH, UNI-WIE
Task 4.1 (M1-M6. Leader CNR, INTERPOL, Partners K&I). Identifying and mapping stakeholders

Task 4.2 (M8-M11. Leader CNR, Partners ALL) – Workshop1: Meeting (duration of 1-2 days depending on the program of the meeting and on the number of stakeholders that will join) the legal community Stakeholder engagement. Inform legal community ALL (prosecutors, law enforcement, judiciary, lawyers, policy advisors) on EIO and e-Evidence, the legal issues involved and the available instruments for technical support and get feedback from them. All partners are invited to join (their travel budget is also calculated taking these costs into consideration) and EAB will be invited as well (Travel budget for them is allocated in the coordinator's travel budget). The location chosen will be the easiest to be reached by all partners and stakeholders and this may lead to a choice of not very cheap venues (i.e Brussels, Amsterdam, The Hague, Vienna).

Task 4.3 (M12-M15, Workshop: Meeting (duration of 1-2 days depending on the program of the meeting and on the number of stakeholders that will join) the Technical community. Leader CNR, Partners ALL). Inform technicians that serve the legal ALL community on the available instruments, what the back office should bring to make use of Evidences and e-CODEX and collect issues surfacing at technical level that require policies and get feedback from them. All partners are invited to join (their travel budget is also calculated taking these costs into consideration) and EAB will be invited as well (Travel budget for them is allocated in the coordinator's travel budget). The location chosen will be the easiest to be reached by all partners and stakeholders and this may lead to a choice of not very cheap venues (i.e Brussels, Amsterdam, The Hague, Vienna).

Figure 1: Extract from the GA on WP4 description, page 21

This project was funded by the European Union's Justice Programme (2014-2020) under Grant Agreement No. 766468

Given the subject matter and timeline proximity, it was decided to merge the WP4 Technical Workshop with the WP3 Final Workshop (D3.3) with digital forensic and legal experts on the formal language for evidence exchange representation. Therefore, a more comprehensive presentation of the technical findings and conclusions pursuant to the event discussions is provided in deliverable D3.3 "Final workshop with digital forensic and legal experts on the formal language for the evidence exchange representation".

This report starts with a general presentation of the event objectives, structure and participants. The report continues with an outline of the event content, covering the essence of the discussions held during the panel sessions and the presentation of WP2 data protection findings, CASE and e-Evidence Digital Exchange System. The deliverable mentions the dissemination efforts undertaken prior to, during and following the event. The report ends with some conclusions and observations made by the stakeholder community regarding the EVIDENCE2e-CODEX activities and the broader goals. For the reader's convenience, the annexes comprise of the:

- event agenda;
- list of participants;
- logistical note;
- template invitation letter.

The appendix contains:

- the updated version of the Report on Task 4.1 "Identifying and Mapping Stakeholders" prepared by Knowledge and Innovation (K&I), dated 25 March 2019.

The PowerPoint presentations made during the event that were authorised for sharing are available for consultation on the project website[1].

[1] https://evidence2e-codex.eu/a/wp4-workshop-2

This project was funded by the European Union's Justice Programme (2014-2020) under Grant Agreement No. 766468

2 Overview

The Technical Workshop dedicated to validating the Evidence Exchange Standard Package Application was a joint WP3/WP4 workshop co-organized by INTERPOL in its capacity as WP4 leader together with the project coordinator CNR-ITTIG and CETIC who are in charge of developing the Evidence Exchange Standard Package (EESP) application and fulfilling the WP3 "Matching EVIDENCE into e-CODEX and Linking to other EU Member States" goals. Within the evidence exchange scenario outlined in this project, the EESP application is to be used by forensic laboratories and law enforcement agencies (LEA) involved in an investigation to prepare the evidence package for its exchange among the Competent Authorities of EIO/MLA Issuing and Executing States.

2.1 Objective

Based on past projects experiences, the consortium acknowledged the importance for practical and results-oriented projects such as EVIDENCE2e-CODEX to receive continuous feedback from end-user representatives as the project unfolds. Within the overall project structure, this is reflected in the fact that a whole work package, WP4, is dedicated to stakeholder engagement, mutual learning and capacity building for professionals, policy makers and technicians.

Given the project's subject matter, aiming to create a legally valid instrument to exchange digital evidence over the e-CODEX, two general types of stakeholders have been identified - technical and legal. The representatives of these stakeholder communities are to be informed on the project developments and findings through the organisation of three WP4 workshops.

A first WP4 workshop dedicated to Stakeholder engagement with the Legal community was held on 15 January 2019 in Brussels.[2] It enabled the consortium

[2] Further information on this available in Deliverable D4.1'Conclusion report and feedback from the first WP4 Workshop dedicated to Stakeholder Engagement with the Legal Community'.

This project was funded by the European Union's Justice Programme (2014-2020) under Grant Agreement No. 766468

to share with prosecutors, judiciary, law enforcement, lawyers, etc. the project's legal research outcomes (i.e. WP2 preliminary findings on EIO and MLA legal implications) and to collect their feedback on the practical realities surrounding EIO implementation, its co-existence with the MLA and to discuss other available instruments.

This follow-up technical workshop "Meeting the technical community to validate the Evidence Exchange Standard Package Application" aimed to engage the technical community with the EVIDENCE2e-CODEX achievements and goals by informing technicians that serve the legal community about available instruments and back office needs for enabling evidence transfer via e-CODEX. The event also enabled the consortium to collect issues surfacing at technical level that require policies and to get feedback from participants on possible solutions.

The meeting sought to share with the representatives of the technical community, the outcomes of Work Package (WP) 3 "Matching EVIDENCE into e-CODEX and linking to other EU Member States" and to collect expert feedback on:

- EESP application demo: Within the evidence exchange scenario outlined in the EVIDENCE2e-CODEX project, the EESP web application is used by forensic laboratories and law enforcement authorities involved in an investigation to create the evidence package and to facilitate its exchange among the competent authorities of EIO/MLA Issuing and Executing States;
- EESP content in detail, including its functionalities and Graphical User Interface (GUI): The EESP application supports the Unified Cyber Ontology (UCO)/Cyber-investigation Analysis Standard Expression (CASE) language;
- Other platforms used for cooperation by LEAs and other competent authorities, including the security and exchange implications;
- Solutions for the exchange of large files of digital evidence;
- Evidence package handling with support for large size files and focus on related legal issues, including data protection, data retention and data disposal considerations.

This project was funded by the European Union's Justice Programme (2014-2020) under Grant Agreement No. 766468

2.2 Structure

To achieve the set objectives, the workshop focused on the EESP application, offering thorough explanations and demos of the tool and covering its different aspects such as architecture, functionalities, use cases, timeline, etc.

This was complemented by five panel discussions:

1. EESP functionalities and GUI features & the integration between the EESP and e-Evidence Digital Exchange System[3];
2. Type of evidences & traces - forensic tool companies, forensic laboratories and Law Enforcement perspective on CASE;
3. Legal aspects for evidence package retention, disposal, grounds for exchange;
4. Exchange of large files of evidence;
5. Other platforms enabling evidence exchange, i.e. INTERPOL I-24/7, Europol SIENA, NFI Hansken.

Lastly, the event incorporated three presentations:

- Overview of the Cyber-investigation Analysis Standard Expression (CASE) language presented by the technical director of the CASE community;
- Update on the status of the e-Evidence Digital Exchange System under the development of the European Commission Directorate-General for Justice and Consumers;
- Findings of deliverable D2.3 "Report on data protection and other fundamental rights issues" prepared by the University of Vienna, which had to be postponed from the legal workshop held in January 2019.

[3] The e-Evidence Digital Exchange System is developed by the European Commission (Directorate-General for Justice and Consumers).

This project was funded by the European Union's Justice Programme (2014-2020) under Grant Agreement No. 766468

2.3 Stakeholders

A key element in the attainment of WP4 objectives and for the successful organisation of WP4 workshops is the identification of appropriate stakeholders. Therefore, the first task in WP4, Task 4.1 led by K&I, concentrated on identifying the different types of stakeholders (i.e. with direct interest, indirect role in the exchange/handling of electronic evidence) that should be involved in the different project activities, not limited to WP4 events. As previously reported, a questionnaire validated by the WP4 partners was circulated among the project consortium to capitalise on the interdisciplinary and international background of partners[4]. The aggregated results were communicated to the consortium. However, following additional input beyond the initial reporting period, K&I shared an updated version of the map in March 2019 comprising a total of 181 potential stakeholders for project involvement. For detailed information on Task 4.1 activities, methodology and results (i.e. typological categories covered, geographical reach) please consult the Task 4.1 report[5] prepared by K&I as well as the updated map.

Based on Task 4.1 findings and given that this was a joint WP3/WP4 event, many of the invited stakeholders have been previously identified for involvement in past EVIDENCE2e-CODEX events, such as the WP3 Interim Workshop with digital forensic and legal experts on the formal language for the evidence exchange representation organised on 20-21 November 2018 or the WP4 Legal Workshop held in 15 January 2019. The workshop experts represented the following categories:

- Digital forensic laboratories (National Forensic Institute);
- Forensic solution providers (Magnet Forensic, MSAB);
- Ministries of Justice technicians (Spain, Italy, Austria, the Netherlands, Bulgaria);
- International organisations (International Criminal Court, INTERPOL);
- National authorities (Bundeskriminalamt, the Metropolitan Police) ;

[4] EVIDENCE2e-CODEX consortium is made of 21 partners, representing 10 Member States.
[5] Report available in Appendix A

This project was funded by the European Union's Justice Programme (2014-2020) under Grant Agreement No. 766468

- EU institutions (Europol, Eurojust, OLAF, EC).

INTERPOL reached out to over 40 experts inviting them to participate in the Technical Workshop dedicated to validating the Evidence Exchange Standard Package Application. As it can be seen from the List of Participants[6], 53 participants attended the workshop including some 20 project partners. One of the panellists was unable to physically join the event due to a conflicting commitment and participated remotely via video connection. To facilitate stakeholders' attendance of the event, including travel and accommodation preparations, the hosting party, the Dutch Ministry of Justice and Security, issued a logistical note[7] that was circulated to all the attendees.

[6] List available in Annex 2
[7] Logistical note available in Annex 3

This project was funded by the European Union's Justice Programme (2014-2020) under Grant Agreement No. 766468

3 Discussions

Welcome

The hosting partners from the Dutch Ministry of Justice and Security opened the event by referring to the 2016 origin of the project proposal - to foster cross-border criminal investigations by connecting the worlds of digital forensic and data exchange via the secure e-CODEX platform. In light of the EC proposal for a European Production and Preservation Order for electronic evidence in criminal matters, there is an even more pressing need to come up with a commonly accepted standard to enable seamless and fast data transfers among countries.

EESP overview

CNR-ITTIG contextualised the EESP application's role by providing an overview of its place within the overall architecture and its wider implications. EVIDENCE2e-CODEX and EXEC projects combine efforts to make possible the exchange of digital evidence among competent authorities of EU Member States in the framework of EIO and MLAs. In this context, the e-CODEX secure platform aims to extend its portfolio of services to digital evidence exchange. The system operates at international level by making it possible to exchange messages between Issuing and Executing States. The EC developed Reference Implementation is optional, as MS are free to adopt their own national solutions, provided it is compliant with the common requirements to ensure interoperability.

The goal of the EVIDENCE2e-CODEX project is to provide for the Evidence Package, both data and metadata components, by ensuring its transparency, and a common standard and understanding by all stakeholders involved in the exchange process. This essential aspect of the process ensures interoperability between countries and tools employed, strengthens evidence admissibility, provides trustworthy information and enables more advanced data analysis. The Evidence Package can be perceived as a locked box where the protected content lists the people involved in the process, their roles, the investigative action, the lifecycle, instruments employed, traces and the relationship among all these elements - setting a chain of custody and chain of evidence. A common standard is required to create and prepare the Evidence Package for its exchange via the

This project was funded by the European Union's Justice Programme (2014-2020) under Grant Agreement No. 766468

system infrastructure (RI & e-CODEX). The choice was made for the Unified Cyber Ontology (UCO)/ Cyber-investigation Analysis Standard Expression (CASE) language, supported by the digital forensic community.

3.1 Presentations

The joint WP3/WP4 workshop "Meeting the technical community to validate the Evidence Exchange Standard Package Application" focused on EESP demos and associated expert discussions. The presentations facilitated the discussions by providing background information to the audience. Below is a brief overview of the three presentations made during the event. As mentioned in the introduction, the PowerPoint presentations authorised for sharing are available for consultation on the project website[8].

3.1.1 CASE overview

Harm van Beek, CASE Technical Director, provided an update on the status of the CASE community since its inception. **C**yber-investigation **A**nalysis **S**tandard **E**xpression (CASE) represents a community-developed standard format meant to serve the needs of the broadest possible range of cyber-investigation domains. It supports the report and exchange of digital traces, as well as tool validation in the context of digital forensic science, incident response, counter-terrorism, criminal justice, forensic intelligence and situational awareness. CASE is defined as a profile of the Unified Cyber Ontology (UCO). In addition to the EVIDENCE2e-CODEX initiative, it also collaborates with other fellow projects that focus on tool validation within digital forensic science.

Initial CASE ideas were presented in 2015 followed by a CASE introduction paper in 2017. In 2018 further to a first roadmap, the community formalization started with agreed needs, a code of conduct, governance and ontology committee elections. Eoghan Casey from the University of Lausanne is the presiding director of the governance committee. As a small organization growing into a professional

[8] https://evidence2e-codex.eu/a/wp4-workshop-2

This project was funded by the European Union's Justice Programme (2014-2020) under Grant Agreement No. 766468

one, much work is still in progress, i.e. the creation of two new committees, a privacy statement, an application form and operation guidelines. An upcoming ontology workshop is scheduled for the summer 2019. Multiple organizations are interested in CASE: NIST (National Institute of Standards and Technology), Cellebrite, IBM, MSAB (Micro Systemation AB), etc. EVIDENCE2e-CODEX represents an important partner given its international and large-scale use of the language. CASE community website www.caseontology.org containing bylaws, meeting notes, documentation with use cases, will be available soon.

A workshop participant expressed support for the CASE standard and urged tool vendors to adopt it. However, the participant also voiced concern that despite all the efforts, including EVIDENCE2e-CODEX, there is a risk that evidence will not be processed in a structured way. This is counterproductive for evidence package exchange between multiple stakeholders, as using a common standard would facilitate the process.

3.1.2 Data Protection and Fundamental Rights issues in the exchange of e-evidence

Professor Nikolaus Forgó from the University of Vienna made a presentation on deliverable D2.3 "Report on data protection and other fundamental rights issues". Deliverable D2.3 was prepared within the scope of EVIDENCE2e-CODEX WP 2 "Legal Issues", examining how data protection implications in EIO and MLA procedures are being handled.

Deliverable D2.3 is structured around the following topics:

- Introduction to Electronic Evidence and Data Protection
- Data Protection Framework
- Mutual Legal Assistance
- European Investigation Orders
- Data Protection in European Investigation Order Procedures
- Data Protection in Mutual Legal Assistance Procedures
- Other Fundamental Rights
- National Implementation

This project was funded by the European Union's Justice Programme (2014-2020) under Grant Agreement No. 766468

- Legislative Developments

Data protection is a fundamental right in Europe that entails more than the protection of personal data, as it includes data security and adjacent limitations of fundamental rights. Deliverable D2.3 studied the distinct scope and application of the General Data Protection Regulation (GDPR) and Directive 2016/680. It considered the necessity of ensuring a high level of data protection, the limitations on fundamental rights, legislative developments and implications for other fundamental rights and national implementation.

The data protection legal framework consists of the EU Charter of Fundamental Rights (Articles 8 and 52)[9], the EIO Directive 2014/41 (Article 20)[10], the Law Enforcement Directive 2016/680 (Article 1, Article 4, Article 29)[11] and the Convention on Mutual Assistance in Criminal Matters between the EU Countries (Article 23)[12]. A considerable challenge is that the majority of the documents constituting the legal framework pertain to a time when technology was much different from nowadays. The fundamental data protection principles that originated in the 1980s are still perceived as abstract by some. Among the more recent approaches are Privacy by Design and Privacy by Default that aid in ensuring data protection adherence. The data protection provisions have different implications in the EIO and MLA environments given the specificities of each instrument. For example, the EIO scope is limited to investigative measures aimed at gathering evidence while the MLA covers wider measures. Data transmissions to third countries are only possible within the MLA, provided the existence of an MLA agreement. The EIO Directive only sets minimum standards in Article 20. However, it also refers to the Council of Europe Convention for the protection of individuals with regard to the Automatic Processing of Personal Data and its Additional Protocol.

[9] EU Charter of Fundamental Rights, *Article 8 Protection of personal data* and *Article 52 Scope and interpretation of rights and principles*
[10] EIO Directive 2014/41, *Article 20 Protection of personal data*
[11] Law Enforcement Directive 2016/680, *Article 1 Subject-matter and objectives, Article 4 Principles relating to processing of personal data* and *Article 29 Security of processing*
[12] Convention of 29 May 2000 on Mutual Assistance in Criminal Matters between the EU countries, *Article 23 Personal data protection*

This project was funded by the European Union's Justice Programme (2014-2020) under Grant Agreement No. 766468

Deliverable D2.3 is a public document that contains checklists of operational and legal measures to ensure compliance with the relevant legislation when exchanging electronic evidence. When processing personal data, taking into consideration these measures helps to ensure legal compliance. Among the examples of operational measures cited is processing only by a competent authority, distinguishing between different categories of personal data and performing data protection impact assessments. The report considers the potential impact on other fundamental rights i.e. effective remedy and fair trial, in the context of EIOs with reference to case law from both the Court of Justice of the EU (CJEU) and the European Court of Human Rights (ECtHR). D2.3 also covers the role of lawyers with regard to EIOs and the transfer of electronic evidence. Further legal issues raised for consideration include security measures, justification of processing, the rights of the data subject and obligations of data controller and processor. A lot of issues related to security are linked with how to justify the different processes and to respect the rights of data subjects.

Finally, D2.3 examines the national implementation situation in four countries – Austria, Bulgaria, France and United Kingdom. The University of Groningen provides additional input in deliverables D2.1 and D2.2 through a broader overview debating the situation in 15 MS. The University of Vienna will provide further input to the work carried out in WP3 with regards to the legal framework for the processing of information. It is important to foster the debate between the legal and technical stakeholders within the EVIDENCE2e-CODEX project, as foreseen in the final WP4 workshop to be held in September 2019. The WP2 findings will continue to guide the work on technological developments undertaken within WP3. For further information, please consult deliverable D2.3.

3.1.3 e-Evidence Digital Exchange system

Djamila Bin-Miloud from the European Commission (EC) presented the latest progress in the development of the e-Evidence Digital Exchange System. The EC is grateful to MS for the feedback provided on the platform's functioning. This is a crucial aspect in ensuring that the platform responds to MS' needs and expectations.

This project was funded by the European Union's Justice Programme (2014-2020) under Grant Agreement No. 766468

To complement the previous demo of the platform from the issuing side, the EC presentation focused on the perspective of an executing authority. Once the EIO form is validated internally and signed off, it is sent to the executing authority which has three possibilities:

- it can reject the EIO request and must provide the ground for refusal;
- if the authority is partially competent to execute the request it can forward it to another Competent Authority within the MS;
- it can execute completely the request by itself.

When an EIO request is accepted, the executing authority has 30 days to return Annex B form – Confirmation of the receipt of an EIO, and 60 days to execute it. The platform is available in all of the EU official languages. However, content in the free text areas of the form remains in the original language as sent. For security reasons, the platform does not foresee access for translators outside the judicial system. The two central components of the platform are the court database and the configuration management tool. The court database for criminal matters is there to facilitate the search and identification of competent authorities. In terms of access management, authentication is based on EU login for MS that do not own a national solution. Currently, a security analysis study is ongoing with preliminary results taking into consideration national parameters and governance. As security aspects are being evaluated, it will be decided if end to end encryption is preferable or point to point encryption provides sufficient protection. The platform should be ready for testing after the Easter holidays 2019, followed by another release this summer with enriched system features and workflow. The MS will be distributed access points to test it and to exchange among themselves. With respect to the national set-up of access points, the EC is offering national support both remotely and on-site. The final release is planned for October 2019.

3.2 Panel Sessions

As detailed in section 2, the purpose and focus of the joint WP3/WP4 Technical Workshop was to present and validate the EESP application through demos and thorough explanations of the tool, its functionalities, uses and scenarios. To this end, the five panel sessions provided suitable ground and momentum for collecting valuable expert feedback on the tool pursuant to these demos, use

This project was funded by the European Union's Justice Programme (2014-2020) under Grant Agreement No. 766468

cases and scenarios. This section provides an outline of the discussion. A comprehensive presentation of the technical features and exchanges is contained in deliverable D3.3 "Final workshop with digital forensic and legal experts on the formal language for the evidence exchange representation".

3.2.1 Panel 1 EESP Application Functionalities & e-Evidence Digital Exchange System

Panellists:

- Fabrizio Turchi, CNR-ITTIG, Italy
- Ray Genoe, Centre for Cybersecurity and Cybercrime Investigation, University College Dublin, Ireland
- Francesco Picasso, Reality Net, Italy
- Mattia Epifani, CNR-ITTIG, Italy
- Claudio Massari, Ministry of Justice, Italy
- Nikolaos Matskanis, CETIC, Belgium
- Djamila Ben-Miloud, European Commission, DG Justice and Consumers
- Huub Moelker, Ministry of Justice and Security, the Netherlands
- Bernhard Rieder, Ministry of Constitutional Affairs, Reforms, Deregulation and Justice, Austria

This panel discussed the different needs that judicial authorities and practitioners would have with the potential handling of the EESP application, such as verifying the content of the evidence package, its authenticity, integrity etc. These needs were contrasted with those of forensic laboratories and law enforcement authorities in their use of the EESP application. The participants highlighted the importance for authorities to work with a standardised validation tool, using the same language in the transnational exchange of evidence packages. Therefore, the EESP was appraised as providing such a means for the exchange of electronic evidence. Some urged for a less technical presentation of the package contents by the interface in order to facilitate the process of validating the packages by non-technical users with the Competent Authority role. Regarding access to the tool, some questioned one of the presented deployment scenarios that included both public and private forensic laboratories as not so pragmatic as typically private laboratories should not be allowed to access applications deployed at the

This project was funded by the European Union's Justice Programme (2014-2020) under Grant Agreement No. 766468

public authority's domain. With exchanges over e-CODEX and the Reference Implementation platform being under the control of competent authorities, they should remain the ultimate decision-makers regarding all access, analysis and collection aspects. For judicial authorities, reliability of evidence, including integrity, trustiness and authenticity, is paramount. Many judicial authorities rely upon long-established relationships with particular, trusted laboratories for raw data analysis. This brings the need to accustom authorities to understand and trust the analysis coming from non-familiar forensic laboratories using the same standards.

Other discussions included the need to define if the application should foresee a potential role for analytics in the future, and deciding upon a satisfactory level of encryption, ensuring security and integrity of the file without being too cumbersome for the digital transfer of files. The panel was presented with four potential EESP application use cases to consider how realistic and viable they were. Finally, in order to discuss the interaction of the EESP application with the EC e-Evidence Digital Exchange System, following an update from the EC on the status of its development (see section 3.1.3), the panellists discussed the needs of forensic laboratories, law enforcement and competent authorities of Issuing and Executing States based on two scenarios. First, from an Executing State perspective, the needs of a competent authority that has to receive the evidence package internally from a forensic laboratory/LEA via the Reference Implementation or national solution if existent. Second, the needs of a forensic laboratory/LEA that obtained the evidence package from an Issuing State. The EESP manifest file content, size as well as encryption aspects, including asymmetric cryptography, were discussed in detail.

3.2.2 Panel 2 CASE: Forensic tool companies, forensic labs and LEA perspectives

Panellists:

- Mattia Epifani, CNR-ITTIG, Italy
- Eoghan Casey, University of Lausanne, Switzerland
- Martin Westman, MSAB, Sweden
- Hans Henseler, Magnet Forensics, the Netherlands

This project was funded by the European Union's Justice Programme (2014-2020) under Grant Agreement No. 766468

- Fabrizio Turchi, CNR-ITTIG, Italy
- Harm van Beek, NFI / CASE Technical Director, the Netherlands
- Nikolaos Matskanis, CETIC, Belgium

Following the overview presentation of the CASE community by its technical director Harm Van Beek (see section 3.1.1), the panel deliberated the standard's acceptance from the perspective of forensic tool software companies. According to some, following initial hype surrounding the standard's launch, currently more vendors and developers need to be convinced to adopt it. Time constraints represent a challenge that could be addressed with the support of a convertor tool that would help with translation in both exporting and ingesting features. A closer look was taken at the CASE functionality, in particular the companies shared their view on the chain of custody and the chain of evidence which are crucial aspects in the scope of EIO and MLA exchange. They discussed the responsibility for developing and maintaining the CASE standard and supporting tools. Finally, the most common type of traces and the CASE short and mid-term perspectives were discussed. The presiding director of the CASE community, Eoghan Casey, who joined the panel discussions remotely, expressed hope that the community will continue to work together to develop the language by addressing existing issues and further defining traces, which will ultimately result in increased interest in the standard on behalf of digital tool developers.

3.2.3 Panel 3 Legal issues, data protection and other concerns

Panellists:

- Nikolaus Forgó, University of Vienna, Austria
- Teresa Magno, Eurojust-Italy
- Jorge Espina, Eurojust-Spain
- Julia Antonova, Ministry of Justice, Estonia
- Ianina Lipara, European Judicial Network
- Fabrizia Bemer, Ministry of Justice, Italy

This project was funded by the European Union's Justice Programme (2014-2020) under Grant Agreement No. 766468

The panellists discussed:

a) the data retention provisions applicable to the evidence package;

b) whether data can be kept in the information systems of forensic laboratories and law enforcement authorities in addition to that of competent authorities;

c) whether different rules apply for forensic laboratories, law enforcement and competent authorities' local systems;

d) issues surrounding evidence package disposal and most suitable means of disposal.

According to national data retention laws, the copies of incriminating files are stored with the case file until a judgement decision is pronounced. Evidence can be stored as long as there is legal ground pursuant to the criminal proceedings. Recent Italian legislation prescribes for specific timeframes for data processed in relation to prosecution. For example, the evidence package concerning a convicted person can be retained for 25 years from the date of the final decision. With regards to the issue of electronic copies of seized data, the Estonian national law does not detail the scientific methods to be used. It was expressed that no specific procedural rules concern digital evidence as opposed to non-digital evidence. Whereas some countries move into fully digitalised proceedings, where the whole criminal file will soon amount to electronic evidence, other MS do not have advanced digital procedures in place and still require implementing legislation. As evidence can also be physical, a suggestion was made for the e-Evidence Digital Exchange platform to consider adding a barcode to the package containing physical evidence to facilitate its tracing. Also, it would facilitate the work of involved stakeholders if videoconference hearings, currently run through a separate dedicated platform, could be linked to the e-Evidence Digital Exchange infrastructure.

Referring to the example of the e-CODEX infrastructure, to join it, the Ministry of Justice of a given country must sign a "Circle of Trust" Agreement establishing a legal basis to recognise exchanged electronic information. Thus, participating countries accept what is legally valid in other participating countries for the content of documents, information on identity and signatures. The workshop participants do not consider that the evidence exchange scenario under development requires a separate legal ground to be accepted. In Italy, an EIO can be handled by LEAs. However, it requires the validation of a prosecutor. Questions arose as to the access to the platform of third parties involved in the

This project was funded by the European Union's Justice Programme (2014-2020) under Grant Agreement No. 766468

investigation, such as lawyers. Regarding translation, it was noted that many countries do not accept automatic translation and it would be useful for official translators working for a court to also access the system. Since judicial cooperation requests entail lots of sensitive data, it is important to ensure that third parties handling such information respect established privacy procedures. Moreover, translation poses serious challenges with regard to time, causing extra delays, costs and accuracy concerns. An option evoked to overcome translation challenges associated with delays and costs is adopting a single common language.

Although not expressing a country perspective, the European Judicial Network (EJN) collects data from practitioners, judges and prosecutors, representing Ministries of Justice that facilitate judicial cooperation. The EJN provides its feedback to EU bodies and institutions for incorporation into their work. The EJN contact points are supportive of the EVIDENCE2e-CODEX project and believe that digital evidence integrity and preservation need to be factored in the development of the platform. To enable the work of stakeholders, the platform needs to provide clear instructions as who should receive the information requests and how to identify and contact a competent authority on the receiving side. In this regard, the EJN highlighted a number of useful tools for practitioners i.e. Fiches Belges, Atlas database. Some misunderstanding persists on the part of MS as to the function of EIO. Some confuse it with rotatory letters or freezing orders. Therefore, it was suggested linking the system with useful sections of EJN websites to ease practitioners' guidance through the system i.e. the instrument to be used, the interpretation of a measure in different countries, etc. Representatives of both the EJN and Eurojust expressed interest in being connected to the e-Evidence Digital Exchange system.

Reminding of the judicial cooperation framework in the EU, which is based on the EIO and Convention 2000, all actions undertaken must comply with these legal instruments that take into consideration data protection requirements. The data retention timeframes are defined by the national criminal procedural rules. The technology should serve the national criminal procedure needs, as the platform is meant to facilitate the exchange of digital evidence. Therefore, it is important to remember that the system must be led by judicial authorities by connecting directly the individuals concerned. In compliance with the applicable legal framework, national judicial authorities should have the prerogative to decide

This project was funded by the European Union's Justice Programme (2014-2020) under Grant Agreement No. 766468

which experts are authorized to connect to the system. The system must enable an executing authority to access the content of an evidence package prepared by a forensic laboratory as it may contain grounds for non-recognition of an EIO, if it affects national security for example. It is important for the system to be as simple and as user-friendly as possible, otherwise it risks not being used by concerned authorities since it is not compulsory.

The audience was concerned that there is no legal or at least soft law instrument prescribing the use of e-CODEX as this may result in countries not using it and undermining the usefulness of the whole e-Evidence Digital Exchnage infrastructure which is useful as long as all/most countries use it. Panellists agreed that ease of use is one of the primary drivers in ensuring the endorsement of a voluntary instrument. Pending a legal solution, a promotional video could induce countries to adopt e-CODEX by explaining its added-value of guaranteeing a secure transmission in the EIO context.

3.2.4 Panel 4 Exchange of large files of evidence

Panellists:

- Djamila Ben-Miloud, European Commission, DG Justice and Consumers
- Fabrizio Turchi, CNR-ITTIG, Italy
- Mattia Epifani, CNR-ITTIG, Italy
- Nikolaos Matskanis, CETIC, Belgium
- Ray Genoe, Centre for Cybersecurity and Cybercrime Investigation, University College Dublin, Ireland
- Valentin Gatejel, OLAF

The project team presented overall two scenarios for transferring of large files that uses: a) a small-sized evidence data file, less than 2 gigabytes, with data and meta-data including a web reference to the physical file, encrypted; b) a larger evidence file, containing the physical file, encrypted and saved on a storage area that is sent separately from the meta-data accessible via web reference. The panel deliberated the advantages and disadvantages of each of the proposed solutions. It was noted that the average size of evidence files

This project was funded by the European Union's Justice Programme (2014-2020) under Grant Agreement No. 766468

continues to grow, with the latest statistics indicating that files close to two terabyte worth of data per person were generated during an investigation. Therefore, a solution for the transmission and storage of large files is required nowadays, even more so in view of the EC proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters which will entail the transfer of big volumes of data. Referring to their day to day realities of handling large files of evidence, judicial authorities reminded that in practice electronic data is transferred physically once copied on an external device. Sometimes it is the raw data that is transferred in order to respect the other country's request.

The discussions covered the usual evidence file size requirements and the desired timeframe to make the evidence files available. To answer the last issue, the parties invoked average procedure timeframes at institutional level. The participants underlined the difference between the legal considerations for data retention of the evidence itself and the timeframe during which it needs to be downloaded by a forensic laboratory. With respect to encryption, such average data sizes require considerable time both when uploading and downloading the file, which is an obstacle to the operational time requirements. The advanced solutions need to be acceptable to the respective competent authorities.

Among the considerations suggested is splitting the evidence package and the use of torrent technology, which raised further security questions. The use of a national cloud is another option, having the underlying issue of spreading trust among stakeholders. An alternative previously discussed is a common cloud storage at European level under EC responsibility. It raised criticism as it may be difficult to convince MS to confine data on a cloud storage outside their control. For admissibility, one needs to ensure that the file was validated by the sender and receiver and that the used transmission channel as well as the file itself is secure, and that every action done to the file is logged. Some agreed on the need to encrypt the file and transfer larger files by courier with metadata shared via a secure channel. Among the identified challenges is handling access controls including having different valid users and the divergent timeframes. In addition, the admissibility requirements for the evidence file need to be taken into account as for some MS file compression equals to evidence tampering. It would be useful to first identify all MS admissibility requirements in order to articulate and integrate them into the solution. This would entail studying the possibility of storing the data on a commercial, national or EC supported cloud.

This project was funded by the European Union's Justice Programme (2014-2020) under Grant Agreement No. 766468

From a technical perspective, the split and joint mechanism that provides for gateway and access points, faces limitations at MS level at the entry point of national infrastructure. Apart from the technical constraints and limitations, some of the biggest challenges are the need to consolidate the legal and business organizational requirements of MS, such as finding common solutions to audit needs and legal archives. If there are potential technical solutions to be envisioned, MS need to reconcile their legal, technical and administrative preferences and requirements. The proposed solution should to take into consideration the needs of the executing authority to be able to verify the content of the reply to an EIO request including confirming compliance with matters of national security. SIENA was mentioned as a swift means for exchanging judicial evidence. However, its use should be within the control of competent authorities, otherwise the evidence used in trial can be vulnerable to challenges. In addition to the transfer of files, the platform should enable its sharing among multiple authorities and the need for multilateral assistance should be integrated, exploring the possibility for the tool to be used by Joint Investigatory Teams (JITs). Finally, the potential role for torrent and blockchain technology was considered. It was reiterated that it is important for the solution to be future proof as technology evolves incrementally.

3.2.5 Panel 5 Other platforms in use for the evidence exchange

Panellists:

- Fabrizio Turchi, CNR-ITTIG, Italy
- Christian Foerster, Federal Criminal Police Office, Germany
- Peter Boven, EUROPOL
- Rachida Rodriguez, INTERPOL
- Harm van Beek, Netherlands Forensic Institute, the Netherlands
- Gregory Webb, London Metropolitan Police Service, UK

This panel considered how other existing platforms exchange digital evidence. Particularly, it discussed the different issues dealt with by the platforms, common

This project was funded by the European Union's Justice Programme (2014-2020) under Grant Agreement No. 766468

difficulties faced, solutions proposed and future perspectives. The London Metropolitan Police representative provided examples of CASE use in forensic methods, including forensic analysis of an unsupported file system and semi-automatic validation of forensic tools. Reference was also made to the European Network of Forensic Science Institutes (ENFSI) "IT forensic tools test and validation database" (ValiD) project, including the interpolation of results and tests between forensic laboratories in Europe and third party validation of test sets and results. The participants found the project highly pertinent in light of the growing need for validation.

The German Federal Police representative introduced a research project focusing on real time transmission of lawfully intercepted communications for international investigative purposes. Involving some 20 countries, EU MS alongside US and Australia, the project was launched at the same time as the e-CODEX initiative. The project contains a substantial legal component. It covers different sources of evidence, such as forensic, Wi-Fi hotspots and images. In view of the increased use of encrypted communication means, some participants evoked the need to reconsider the material scope of lawful interception to cover the emerging technological means. The project could potentially envisage the use of the EESP application.

The Europol business product manager presented the Secure Information Exchange Network Application (SIENA), a tool the organization makes available to its members for the exchange of information. SIENA is neither used for actual data storage (Europol information system is in charge of data storage), nor for forensic analysis (Europol analysis system operates forensic analysis). SIENA is primarily (85%) used for bilateral and multilateral exchanges of information with only 15% of its use by MS for exchanges with Europol or third parties. SIENA is accessed by 27 MS, 17 third countries, 14 EU and international organizations with over a million messages processed last year. Although SIENA was not designed to support the exchange of evidence as its main purpose, it presents some elements of relevance in the context of evidence handling and exchange:

- Multiagency approach: since Europol applies a multi-agency approach, various types of competent authorities, regional or specialized, can make use of SIENA, including potentially judicial authorities;

This project was funded by the European Union's Justice Programme (2014-2020) under Grant Agreement No. 766468

- Indications of use in judicial proceeding: messages in SIENA can include restrictions, known as handling codes, on the possible use of information in the context of judicial proceedings;
- Multiple legal frameworks: SIENA's use is not limited to the Europol legal framework, exchanges authorized in the context of other procedures (i.e. Prüm, Naples, Swedish Initiative, MLA) can be supported;
- Integration possibilities with other systems: SIENA can be used as a web-application but can also be integrated with case management or workflow systems via web services;
- Large file exchange: Europol maintains the so-called Large File Exchange (LFE) tool. However, this solution is currently not integrated with SIENA and is not suitable for bilateral exchange of digital evidence although it is planned to extend its use for handling large files and pieces of evidence, such as copies of seized hardware;
- Support for structured information: SIENA supports the exchange of structured information, exchanging messages and attachments, based on universal message format (UMF) developed through a series of EU-funded projects in order to develop a standardized structure.

INTERPOL representative presented three INTERPOL services:

a) I-24/7 is INTERPOL's global communication platform which facilitates the exchange of messages. In addition to the messaging system, it also provides direct access to the databases, including the operational ones, for authorized users through a unique user authentication.

b) Smart case messaging represents a new INTERPOL initiative that intends to bring structure to the mail system by adding algorithms to process messages for actionable intelligence. Project Stadia[13] represented the first use of private cloud for information hosting. It contained no restricted information only public data relating to integrity on sports.

c) Translation as a service is a tool implemented by INTERPOL for its 194 member countries. Users provided positive feedback, although the tool does not intend to replace official translation, it facilitates the understanding of content.

[13] Established by INTERPOL in 2012 and funded by Qatar, Stadia is a 10-year project that will contribute to policing and security arrangements for the 2022 FIFA World Cup™ in Qatar and will leave a lasting legacy for the world's law enforcement community.

This project was funded by the European Union's Justice Programme (2014-2020) under Grant Agreement No. 766468

Unlike the EU which strives towards further standardization and progress, INTERPOL's work is affected by the split between the desire to innovate on one hand, and the need to support its members lacking basic policing capabilities on the other hand.

The NFI representative introduced the Hansken distributed investigative platform that enables a team to cooperate on a single case as the data is stored on a central location. The portal was designed around three key principles - security privacy and transparency. To meet investigators' expectations, the data model is based on multi-typed traces for storing traces and metadata traces. A considerable challenge is providing sound evidence by keeping in place the chain of custody and chain of evidence. Further to the principle of transparency, all information is contained in the report created by the tool. The platform envisioned integrating data science and artificial intelligence (AI) for the identification of objects and pictures. However, courts are somewhat skeptical of the use of AI as a source of evidence, so they do not welcome its presence in the chain of evidence. For time and resource considerations, the use of advanced technology is useful in processing big amounts of data. However, it becomes more controversial when employed for producing evidence. Some participants expressed a different perspective on the use of AI. As long as the final decision is under human control, an algorithm that processes information to provide preliminary results or an initial indication, does not replace the human and should be acceptable in court. Hansken is not open source, but academic licenses are available for free to universities and commercially to LEAs. In the future, the NFI plans to make the tool available to the wider community by offering its functionalities to other organizations outside the Netherlands for their operation through an open-platform to which other tools can plug into the back-end or as interfaces in the front-end.

This project was funded by the European Union's Justice Programme (2014-2020) under Grant Agreement No. 766468

4 Dissemination

The workshop was widely covered online. Before the event, the workshop was listed among the upcoming events on the project's official website event page and it was announced in the news section. The statement included, as usual, the time and place of the event, the purpose of the workshop and the proposed agenda. The partners shared the event on different social media platforms including INTERPOL's LinkedIn and Twitter accounts[14]. The meeting was also intensely covered on the project's official Twitter page.

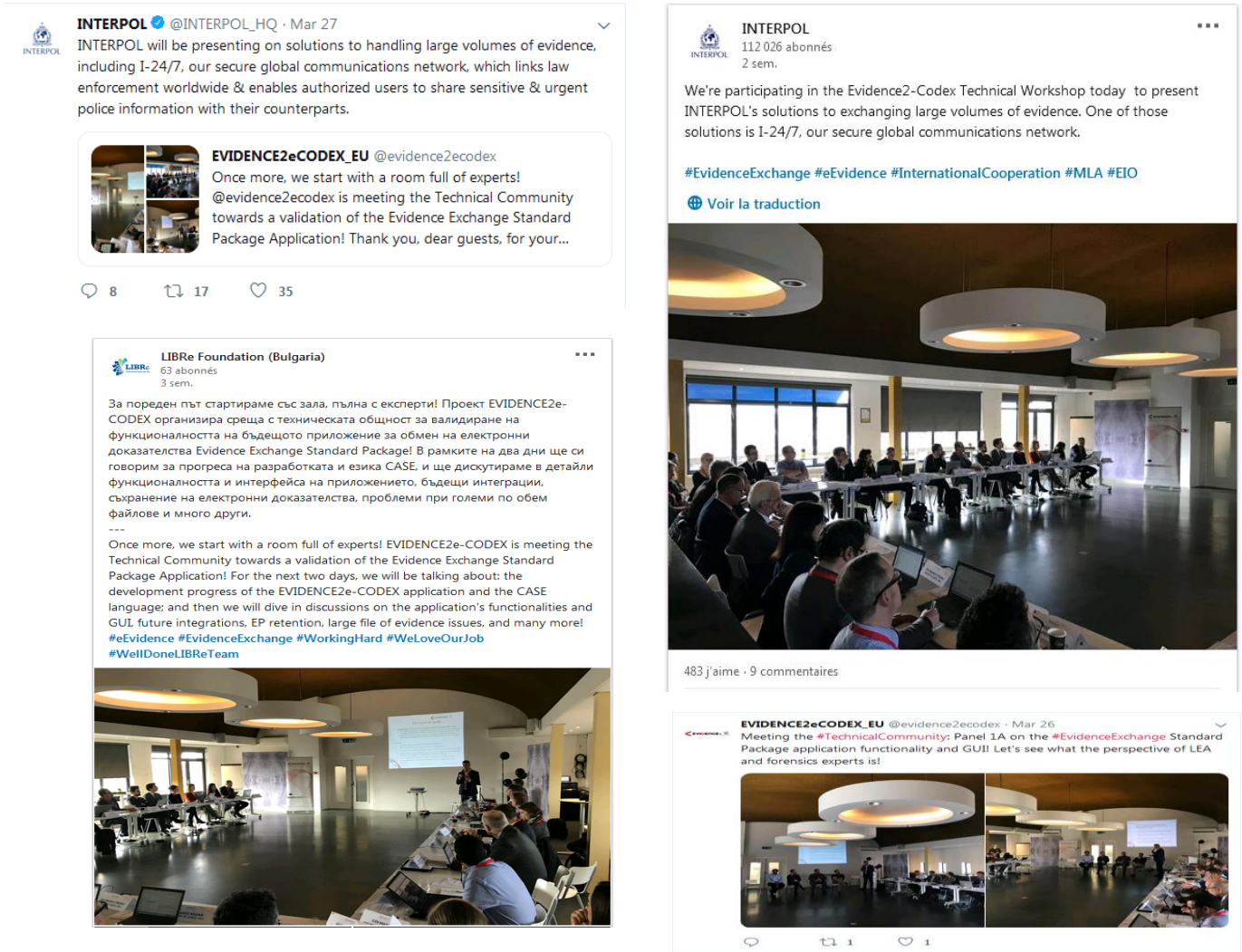


Figure 2-5: partners sharing news of the event on Twitter (figure 2 and 4) and LinkedIn (figure 3 and 5)

[14] INTERPOL's LinkedIn account has more than 110 000 followers, INTERPOL's Twitter – more than 150 000 followers.

This project was funded by the European Union's Justice Programme (2014-2020) under Grant Agreement No. 766468

Following the workshop, a short news report was published on the project's official website. The publication gave an overview of the participants who attended the event and the main discussion topics. It also contained a reference to the event brief which includes a summary of the event and a brief on the EVIDENCE2e-CODEX evidence exchange scenario. Following the event, the page of the event was updated with a summary of the meeting and the main highlights of the workshop.

This project was funded by the European Union's Justice Programme (2014-2020) under Grant Agreement No. 766468

5 Conclusion

The joint WP3/WP4 technical workshop "Meeting the technical community to validate the Evidence Exchange Standard Package Application" provided the opportunity to demonstrate the EESP application and to discuss its content in detail with technical experts in the area, representing both prospective end-users of the tool (competent authorities, forensic laboratories and LEAs), as well as digital forensic tool developers. The meeting enabled the project team to share with the representatives of the technical community the outcomes of Work Package 3 "Matching EVIDENCE into e-CODEX and linking to other EU Member States" and to collect expert feedback. This represents a crucial aspect in the project lifecycle, as it ensures that the developed EESP tool offers a feasible solution that is compliant with the stakeholder needs. In addition to the demo, use cases and scenarios, the workshop enabled the sharing of best practices of other platforms used for cooperation by authorities. The exchanges covered solutions to enable the transfer of large e-evidence files and future perspective on artificial intelligence use and advanced technology measures. The technical discussion integrated a legal component for the technology to be aware of by incorporating a presentation on deliverable D2.3 "Report on data protection and other fundamental rights issues". The legal findings included checklists of operational and legal measures to ensure legal compliance when transferring e-evidence. To complement this legal angle of discussion, a panel debated the wider legal implications of an exchanged evidence package by tackling among other things, the data retention and data disposal provisions which need to be respected by the technology.

As a joint WP3/WP4 event, this workshop benefitted from the expertise of stakeholders identified for engagement in past EVIDENCE2e-CODEX events, such as the WP3 Interim workshop with digital forensic and legal experts on the formal language for the evidence exchange representation and the WP4 Legal Workshop. As a result, the discussions generated a comprehensive appraisal of the EESP by presenting different perspectives and sharing the insights of:

- Digital forensic laboratories;
- Forensic solution providers;

This project was funded by the European Union's Justice Programme (2014-2020) under Grant Agreement No. 766468

- Ministries of Justice technicians (Spain, Italy, Austria, the Netherlands, Bulgaria);
- International organisations;
- National authorities;
- EU institutions.

EVIDENCE2e-CODEX benefited from the shared experience of other existing platforms employed for official exchanges i.e. I-24/7, Hansken, and specific tools such as the Europol Large File Exchange and INTERPOL Translation as a Service. The German Federal Police indicated its potential use of the EESP in the scope of its research project on the transfer of lawfully intercepted information.

The workshop participants were unanimous about the potential benefit of the EESP in facilitating the transnational exchange of evidence packages by enabling authorities to work with a standardised validation tool. The choice of the CASE standard was supported with the need for the language to be further developed and to integrate additional traces. It was agreed that the tool should incorporate all of the MS evidence admissibility requirements in order to present a strong and viable solution. The experts highlighted that the ease of use of the EESP is key to ensuring its uptake as a voluntary instrument by end-users. It is important that the solution put forward is future-proofed as technology evolves incrementally and consideration should be given to the potential role for analytics, blockchain and torrent technology. The feedback provided by end-users and the broader stakeholder community was also incorporated into deliverable D3.3 "Final workshop with digital forensic and legal experts on the formal language for the evidence exchange representation". The consortium processed and analysed the feedback for integration into the future EESP enhancement and for the project's further steering. Preparations are underway for the final WP4 workshop bringing together technical and legal stakeholders to cross-fertilise their views on the project findings and tools.

This project was funded by the European Union's Justice Programme (2014-2020) under Grant Agreement No. 766468

6 Annexes

This project was funded by the European Union's Justice Programme (2014-2020) under Grant Agreement No. 766468

Annex 1: Agenda

JUSTICE PROGRAMME (2014-2020)

JUST-JCOO-CRIM-AG-2016

Action Grants to Support Transnational Projects to Promote Judicial Cooperation in Criminal Matters

Grant Agreement No. 766468

EVIDENCE2E-CODEX

Linking EVIDENCE into e-CODEX for EIO and MLA procedures in Europe

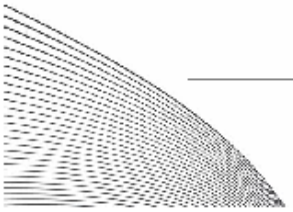
JOINT WP3/WP4 WORKSHOP

MEETING THE TECHNICAL COMMUNITY: VALIDATION OF THE EVIDENCE EXCHANGE STANDARD PACKAGE APPLICATION

26-27 MARCH 2019

Igluu Den Haag

Louis Couperusplein 2, 2514 The Hague, The Netherlands



This project was funded by the European Union's Justice Programme (2014-2020) under Grant Agreement No. 766468

1/4

Annex 2: List of Participants

JUSTICE PROGRAMME (2014-2020)

JUST-JCOO-CRIM-AG-2016

Action Grants to Support Transnational Projects to Promote Judicial Cooperation in Criminal Matters

Grant Agreement No. 766468

EVIDENCE2E-CODEX

Linking EVIDENCE into e-CODEX for EIO and MLA procedures in Europe

JOINT WP3/WP4 WORKSHOP

MEETING THE TECHNICAL COMMUNITY: VALIDATION OF THE EVIDENCE EXCHANGE STANDARD PACKAGE APPLICATION

26-27 MARCH 2019

(excerpt)

Igluu Den Haag

Louis Couperusplein 2, 2514 The Hague, The Netherlands

This project was funded by the European Union's Justice Programme (2014-2020) under Grant Agreement No. 766468

1/8

Annex 3: Logistical Note

Logistical note

EVIDENCE2e-CODEX meeting
26/27 March 2019 The Hague

Meeting venue

The meeting venue is located close to the city center of The Hague.

Address
Igluu
Louis Couperusplein 2
2514 HP Den Haag

Public transportation to meeting venue
From The Hague Central Station
Take tram 9 (direction: *Noorderstrand)* and exit at the second stop (*Dr. Kuyperstraat*)

You can also take a nice stroll from The Hague Central Station to the meeting venue (about half an hour walk).

This project was funded by the European Union's Justice Programme (2014-2020) under Grant Agreement No. 766468

Annex 4: Invitation Letter

INTERNATIONAL CRIMINAL POLICE ORGANIZATION
ORGANIZACIÓN INTERNACIONAL DE POLICÍA CRIMINAL

INTERPOL

ORGANISATION INTERNATIONALE DE POLICE CRIMINELLE
المنظمة الدولية للشرطة الجنائية

Invitation

Date 22 February 2019

Our Ref. LA/71135-1/5.5/JB/XB/tsa

Contact name
Contact title
Institution

Subject **Evidence2e-CODEX "Meeting the technical community: Validation of the Evidence Exchange Standard Package Application" on 26-27 March 2019, The Hague, the Netherlands**

Dear Ms./Mr.,

INTERPOL is participating in the EVIDENCE2e-CODEX research project aiming to facilitate the exchange of electronic evidence within the European Union and to enable international cooperation in the criminal sector. The project seeks to create a legally valid instrument to exchange digital evidence over the e-CODEX in the framework of mutual legal assistance (MLA) and European Investigative Order (EIO) procedures.

Funded by the European Union and conducted by a multidisciplinary international consortium, EVIDENCE2e-CODEX is based upon the results of two completed EU-funded projects - EVIDENCE and e-CODEX. EVIDENCE2e-CODEX will pilot these projects' findings in real-life criminal justice use cases with the support of participating Ministries of Justice.

One of the project objectives is to ensure stakeholder engagement, mutual learning and capacity building for professionals, policy makers and technicians. To this end, the EVIDENCE2e-CODEX consortium will be organising a series of workshops that seek to provide stakeholders from the legal and technical communities with 'ready for use' information on EIO, electronic evidence and e-CODEX.

In this context, it is our pleasure to invite you on behalf of the project consortium to participate in the event dedicated to **"Meeting the technical community: Validation of the Evidence Exchange Standard Package Application"**. The event will be hosted by the Dutch Ministry of Justice, on 26-27 March 2019 at Igluu Den Haag, in The Hague, the Netherlands.

The aim of the meeting is to share with the representatives of the technical community, the outcomes of Work Package 3 "Matching EVIDENCE into e-CODEX and linking to other EU Member States" and to collect expert feedback on:

- Evidence Exchange Standard Package (EESP) application demo. EESP is a web application for creating the evidence package and facilitating its exchange;
- EESP content in details, including its functionalities and Graphic User Interface (GUI). The EESP application supports the Unified Cyber Ontology (UCO)/ Cyber-investigation Analysis Standard Expression (CASE) language;

INTERPOL For official use only Page 1/2

General Secretariat - Secrétariat général - Secretaría General - الأمانة العامة
200 Quai Charles de Gaulle | 69006 Lyon | France | T. +33 4 72 44 70 00 F. +33 4 72 44 71 63 | www.interpol.int

Appendices

A. Updated version of the Report on Task 4.1 "Identifying and mapping stakeholders"

This project was funded by the European Union's Justice Programme (2014-2020) under Grant Agreement No. 766468

EVIDENCE2e-Codex Linking EVIDENCE into e-CODEX for EIO and MLA procedures in Europe

WP4: Stakeholder engagement, Mutual learning and Capacity Building for professionals, Policy makers and technicians
Task 4.1: Identifying and mapping stakeholders

EVIDENCE2 e-CODEX
Linking EVIDENCE into e-CODEX for EIO and MLA procedures in Europe

Questionnaire

Introduction

This online questionnaire is addressed to the partners of the project EVIDENCE2e-CODEX. One project action is to identify and map the stakeholders to be involved in the subsequent activities.

Each project partner is kindly invited to fill out this questionnaire, aimed at identifying specific organizations or individuals considered particularly important to involve in EVIDENCE2e-CODEX workshops and / or in other project initiatives. As it will be seen, these stakeholders are classified, conventionally, in the following manner:

- *Stakeholders having a direct role (for professional reasons) in handling and exchanging electronic evidence; within this category, we can consider broadly two large "communities", that is the "legal community" and the "technical community";*
- *Stakeholders being part of a broader political, social, cultural, economic context influencing the use and the exchange of electronic evidence.*

The person who fill the questionnaire is invited to go to the Checklist, to identify the types of stakeholders on which (s)he believes (s)he can provide information (many or few does not matter), to click on each type of these stakeholders, and fill in one or more forms with the requested information. Of course, the person filling can skip the questions (s)he cannot answer.

In order to comply with the new General Data Protection Regulation (GDPR) consent requirement, prior to completing the questionnaire, the **respondent should first confirm with the potential stakeholder(s) its/their consent** to have their details shared with the Evidence2e-Codex consortium for the purpose of being considered for engagement in the project events and activities. The stakeholder can withdraw its consent at any time by emailing mezzana@knowledge-innovation.org. The name of the questionnaire respondent and all the data collected is treated confidential and will only be used for the purposes of this project. The data will be kept until the survey is completed and at a maximum until the project ends in November 2019.

(Please fill in the fields below and go to checklist)

Respondent's Name:	...
Partner's Name:	...

Go To Checklist

SELECT THE STAKEHOLDE

Stakeholders having a direct role in handling and exchanging electronic evidence
Legal community
1. Public Prosecutors
2. Judges
3. Lawyers
4. Specialized international institutions (INTERPOL, International Criminal Court, etc.)
5. LEAs of EU MS and Intelligence agencies
6. Specialized EU bodies and agencies (EUROJUST, EUROPOL, OLAF-Digital Forensic Unit, DPO, etc.)
Technical community
7. Digital Forensic Software companies (DFSC)
8. Digital Forensic Hardware producers (DFHP)
9. Internet Service Providers / Tech companies (ISP)
10. Forensic examiners (FE)

21. C

:RS FROM THE CHECKLIST

Stakeholders being part of a broader political, social, cultural, economic context influencing the use and the exchange of electronic evidence
11. Policy makers at national level (PMnl)
12. Ministries of Justice of UE MS (Min)
13. UN agencies concerned with justice and technological innovation (UNODC, ECOSOC, etc.)
14. Policy makers at European level (PMel)
15. Other on-going EU Projects
16. Legal and forensic associations and networks
17. Research bodies, associations and networks
18. Actors involved in the field of human rights
19. Scientific and technical journals and web sites
20. The media (mass media, blogs, social networks, etc.)

)ther

	1	Public Prosecutors						
		Name of organization	**Geographical reach**	**Town**	**Country**	**Contact Person**	**e-mail address**	**To be invited to Project workshops**
D1	1	Public Prosecution Service Cologne - Unit for Cybercrime	Local	Cologne	GER	Angela Flierl	angela.flierl@sta-koeln.nrw.de	Yes
A1	2	Prosecutors's office Bulgaria	National	Sofia	Bulgaria		prbcont@prb.bg	Yes
B1	3	Cybercrime Office within the Prosecutor General's Office	National	Lisbon	Portugal	Pedro Verdelho	Pedro.Verdelho@pgr.pt	Yes
C1	4	Staatsanwaltschaft Wien	National	Vienna	Austria	Leitende Staatsanwältin		Yes
C2	5	Oberstaatsanwaltschaft Wien	National	Vienna	Austria	Erster Oberstaatsanwalt		Yes
C3	6	Generalprokuratur	National	Vienna	Austria	Generalanwalt Dr. Martin Ulrich	generalprokuratur@justiz.gv.at	Yes
F1	7	Corte di Cassazione	National	Rome	Italy	Giuseppe Corasaniti	giuseppe.corasaniti@giustizia.it	
G1	8	Ministry of Justice of Italy	National	Milan	Italy	Francesco Cajani	francesco.cajani@giustizia.it	Yes
G2	9	Ministry of Justice of Italy	National	Rome	Italy	Eugenio Albamonte	eugenio.albamonte@giustizia.it	Yes
G3	10	Ministry of Justice of Italy	National	Rome	Italy	Edmondo de Gregorio	edmondo.degregorio@giustizia.it	Yes
G5	11	Ministry of Justice of Italy	National	Rome	Italy	Marco Alma	marco.alma@giustizia.it	Yes

G6	12	Ministry of Justice of Italy	National	Florence	Italy	Nicola Russo	nicola.russo@giustizia.it	Yes
H1	13	Spanish Prosecutor office	National	Madrid	Spain	Borja Jimenez	borja.jimenez@fiscal.es	Yes
Q2	14	Prosecution			Norway	Eirik Tronnes Hansen	eirik.tronnes.hansen@politiet.no	
Q1	15	Public Prosecutor's Office of Amsterdam			The Netherlands	Irene C. van der Ben	i.c.van.der.ben@om.nl	

	Back to cheklist
To be involved in other Project initiatives	**Note**
No	
Yes	
Yes	Pedro Verdelho is the Coordinator of the Cybercrime Office within the Prosecutor General's Office and is the national representative of Portugal in the T-CY Committee of the Council of Europe. At the Committee's Plenary meeting, on 9 July at the Council of Europe, in Strasbourg, he was elected to the Vice-Presidency of the Committee.
Yes	
Yes	fax, see website (https://www.justiz.gv.at/web2013/
Yes	
	Procura Generale
Yes	It will be our job to contact him by Mariangela
Yes	It will be our job to contact him by Mariangela
Yes	
Yes	

Yes	
Yes	

2	Judges						
	Name of organization	**Geographical reach**	**Town**	**Country**	**Contact Person**	**e-mail address**	**To be invited to Project workshops**
16	Supreme Judicial Council	National	Sofia	Bulgaria		vss@vss.justice.bg	Yes
17	National Institute of Justice	National	Sofia	Bulgaria		nij@nij.bg	Yes
18	Österreichische Richtervereinigung	National	Vienna	Austria	Die Präsidentin	sekretariat@richtervereinigung.at	Yes
19	European Networks of Councils for the Judiciary (ENCJ)	Regional	Brussels	Belgium	Monique van der Goes	monique.vandergoes@encj.eu	Yes

	Back to cheklist
To be involved in other Project initiatives	**Note**
Yes	
Yes	
Yes	
Yes	

	3	Lawyers						
		Name of organization	**Geographical reach**	**Town**	**Country**	**Contact Person**	**e-mail address**	**To be invited to Project workshops**
G1	20	Freelancer	International	Milan	Italy	Giuseppe Vaciago	giuseppe.vaciago@uninsubria.it	Yes
G2	21	Freelancer	International		Italy	Stefano Aterno	stefano@aterno.it	Yes
G3	22	Freelancer	International		Italy	Donato La Muscatella	donato.lamuscatelle@hotmail.it	Yes
G4	23	Freelancer	International		Italy	Bruno Fiammella	studiolegale@fiammella.it	Yes
A1	24	Supreme Bar Council	National	Sofia	Bulgaria		arch@vas.bg	Yes
A2	25	Union of the Jurists in Bulgaria	National	Sofia	Bulgaria	Mariana Yaneva	mianeva@sub.bg	Yes
C1	26	ÖsterreichischerTRechtsanwaltskammertag	National	Vienna	Austria	Dr. Rupert Wolff	rechtsanwaelte@oerak.at	Yes
C2	27	Rechtsanwaltskammer Wien	National	Vienna	Austria	Univ.-Prof. Dr. Michael Enzinger	kanzlei@rakwien.at	Yes
F1	28	The Norwegian Police University College/ Arsforensica NTNU	National		Norway	Jul Fredrik Kaltenborn	Jul.Fredrik.Kaltenborn@phs.no	
E1	29	Peter Homoki	Regional	Budapest	Hungary		peter.homoki@homok[illegible]	Yes
E2	30	Jiri Novak	Regional	Prague	Czech Republic		novak@akbsn.eu	Yes
E3	31	Iain Mitchell QC	Regional	Edinburgh	United Kingdom		igmitchell@easynet.co.uk	Yes
E4	32	Mathias Preuschl	Regional	Vienna	Austria		preuschl@phhv.at	Yes
E5	33	Hans Graux	Regiona	Brussels	Belgium		hans.graux@timelex.eu)	Yes
Q1	34	Fair Trials - Belgium				Laure Baudrihaye-Gérard	laure.baudrihaye@fairtrials.net	
Q2	35	European Data Protection Board				Romain Robert	romain.robert@edpb.europa.eu	

Q3	36	CCBE - Criminal Law Committee				James MacGuill	James.MacGuill@macguill.ie	
Q4	37	Austrian Bar Association			Austria	Britta Kynast	kynast@oerak.at	
Q5	38	German Bar Association			Germany	Annegret Kempf	kempf@eu.anwaltverein.de	
Q6	39	CCBE - Criminal Law Committee				Nathalie Boudjerada Natali	nbavocat@icloud.com	
Q7	40	ÖRAK			Belgium	Jessica König	koenig@oerak.at	
Q8	41	CCBE				Peter McNamee	mcnamee@ccbe.eu	
Q9	42	CCBE				Nathan Roosbeek	roosbeek@ccbe.eu	
Q10	43	CCBE IT Law Committee				Greg Ryan	greg@ryansol.com	
Q11	44	DBF				Mathilde Thibault	mathilde.thibault@dbfbruxelles.eu	
Q12	45	German Federal Bar			Germany	Astrid Gamisch	astrid.gamisch@brak.eu	
Q13	46	German Federal Bar			Germany	Hanna Petersen	Hanna.Petersen@brak.eu	
Q14	47	Czech Bar Association in Brussels			Czech Republic	Mgr. Alžběta Recová	Recova@cak.cz	

	Back to cheklist
To be involved in other Project initiatives	**Note**
Yes	
Yes	
Yes	
Yes	President of Austria's chamber of lawyers
Yes	
	Assistant Professor/PhD-fellow
Yes	
Yes	
Yes	
Yes	
Yes	
	Senior Lawyer (Law & Policy), Fair Trials
	Legal advisor – EDPB Secretariat

	Lawyer – Chair of CCBE Criminal Law Committee
	Lawyer - Head of Brussels Office (ÖRAK - Austrian Bar)
	Policy Officer for European Affairs to the German Bar Association (Deutscher Anwaltverein Büro Brüssel
	Lawyer – Member of the CCBE Criminal Law Committee
	Intern
	Senior legal advisor
	Legal trainee
	Sollicitor
	Legal advisor
	Legal advisor
	Lawyer

	4	Specialized international institutions						
		Name of organization	**Geographical reach**	**Town**	**Country**	**Contact Person**	**e-mail address**	**To be invited to Project workshops**
F2	48	International Criminal Court	International	The Hague	Netherlands	Ilyoung Hong	Ilyoung.Hong@icc-cpi.int	
G1	49	ICC	International	The Hague	The Netherlands	Crsitina Ribeiro	cristina.ribeiro@icc-cpi.int	Yes
G2	50	ICC	International	The Hague	The Netherlands	Ilyoung Hong	Ilyoung.Hong@icc-cpi.int	Yes
G3	51	ICC	International	The Hague	The Netherlands	Martin Salgado, Elena	Elena.MartinSalgado@icc-cpi.int	Yes
G4	52	ICC	International	The Hague	The Netherlands	Yvan Cuypers	Yvan.Cuypers@icc-cpi.int	Yes
G5	53	ICC	International	The Hague	The Netherlands	Charlotte Dahuron	Charlotte.Dahuron@icc-cpi.int	Yes
G6	54	ICC	International	The Hague	The Netherlands	Beresford, David	David.Beresford@icc-cpi.int	Yes
G10	55	DoD Cyber Crime Center (DC3)	International		USA	Ryan Griffith	ryan.griffith.ctr@dc3.mil	Yes
Z16	56	INTERPOL	Regiona	Lyon	France	Vincent Danjean	v.danjean@interpol.int	
Z17	57	INTERPOL	Regiona	Lyon	France	Rachida Rodriguez	R.RODRIGUEZ@INTERPOL.INT	

	Back to cheklist
To be involved in other Project initiatives	**Note**
	Cyber forensics investigator
Yes	
	Head of Branch Information Security
	IT Project Manager

	5	LEAs of EU MS and Intelligence agencies						
		Name of organization	**Geographical reach**	**Town**	**Country**	**Contact Person**	**e-mail address**	**To be invited to Project workshops**
C2	58	Landespolizeidirektion Wien	Local	Vienna	Austria		LPD-W@polizei.gv.at	Yes
A1	59	National Investigation Service	National	Sofia	Bulgaria		nsls@nsls.bg	Yes
A2	60	Directorate-General of The Ministry of the Interior for fight against organised crime	National	Sofia	Bulgaria		gdbop@mvr.bg	Yes
B1	61	Criminal Police (Polícia Judiciária) - National Cybercrime Unit (UNC3T)	National	Lisbon	Portugal	Rogério Bravo	r.bravo@pj.pt	Yes
C1	62	Bundesamt für Verfassungsschutz und Terrorismusbekämpfung	National	Vienna	Austria		BMI-II-BVT@bmi.gv.at	Yes
C3	63	Bundeskriminalamt	National	Vienna	Austria		Bundeskriminalamt@bmi.gv.at	Yes
F1	64	Spanish National police	National		Spain	Antonio López	a.lopez@policia.es	
F2	65	Spanish National police	National		Spain	Juan Francisco Benítez Iglesias	jbenitez0000@policia.es	
F3	66	Federal Police Federale Gerechtelijke Politie	National	Asse	Belgium	Koen Smets	koen.smets@fccu.be	
F4	67	International Cooperation Bureau	National		Latvia	Aleksandra Tukisa	aleksandra.tukisa@vp.gov.lv	

Z9	68	Bundeskriminalamt (Federal Cr	National		Germany	Christian Foerster	christian.foerster05@bka.bund.de	
Q1	69	State Police - Latvia			Latvia	Mārcis Laiviņš	marcis.laivins@vp.gov.lv	

	Back to cheklist
To be involved in other Project initiatives	**Note**
Yes	E-Mail adresses of the 8 other police departments auf Austria's regions via http://www.polizei.gv.at/alle/kontakt.aspx
Yes	
Yes	
Yes	Chief Inspector in the UNC3T
Yes	
Yes	
	Subinspector in the Cyber Crime Unit
	Rechercheur / Hoofdinspecteur van politie Regional Computer Crime Unit - *involvement conditional upon autorization from hierarchy*
	Head of 1st Unit

	Erster Kriminalhauptkommissar (EKHK)
	Senior inspector, Central Criminal Police department, International Cooperation department, 3rd unit

	6	Specialized EU bodies and agencies						
		Name of organization	**Geographical reach**	**Town**	**Country**	**Contact Person**	**e-mail address**	**To be invited to Project workshops**
E1	70	Fundamental Rights Agency (FRA)	Regional	Vienna	Austria	Jana Gojdosova	Jana.GAJDOSOVA@fra.europa.eu	Yes
F1	71	Europol	Regional	The Hague	The Netherlands	Gregory Mounier	gregory.mounier@europol.europa.eu	
F2	72	European Data Protection Supervisor	Regional	Brussels	Belgium	Lara Smit	lara.smit@edps.europa.eu	
G1	73	OLAF	Regional	The Hague	The Netherlands	Volker EFFENBERG	Volker.EFFENBERG@ec.europa.eu	Yes
G2	74	European Judiacial Network Secretaria	Regional	The Hague	The Netherlands	Janina Gabriela Lipara	ILipara@Eurojust.europa.eu	
Z2	75	Eurojust	Regiona	The Hague	The Netherlands	Martin Gillen	mgillen@eurojust.europa.eu	
Z3	76	Eurojust	Regiona	The Hague	The Netherlands	Vincent Jamin	vjamin@eurojust.europa.eu	
Z4	77	Eurojust	Regiona	The Hague	The Netherlands	Jorge Espina	jespina@eurojust.europa.eu	
G4	78	Eurojust	Regional	The Hague	The Netherlands	Teresa Magno	t.magno@eurojust.eu	Yes
Z1	79	OLAF				Valentin Gatejel	valentin.gatejel@ec.europa.eu	
Z19	80	EUROPOL	Regiona			Rodolphe Roques-Cou	Rodolphe.Roques-Couchot@europol.eur	
Z20	81	EUROPOL	Regiona			Ruth Linden	Ruth.Linden@europol.europa.eu	
Z21	82	EUROPOL	Regiona			Juan De Dios Toledo M	Juan-De-Dios.Toledo-Martinez@europol.	
Z22	83	EUROPOL	Regiona			Peter Boven	peter.boven@europol.europa.eu	
Z23	84	EUROPOL	Regiona			Donatas Mažeika	Donatas.Mazeika@europol.europa.eu	

G7	85	EUROPOL	Regional	The Hague	The Netherlands	Ellermann, Jan	jan.ellermann@europol.europa.eu	Yes
G8	86	EUROPOL	Regional	The Hague	The Netherlands	Drewer, Daniel	daniel.drewer@europol.europa.eu	Yes

	Back to cheklist
To be involved in other Project initiatives	**Note**
Yes	
	Head of Outreach and Prevention, European Cybercrime Centre
	Legal Officer - requested to be informed about the project and its updates, not sure to which extent will be possible to get involved
Yes	
	Project Officer
	Head of the Joint investigations teams, Network Secretariat
	Assistant to the National Member for Spain
Yes	
	Team Leader of the digital forensic
opa.eu	European Counter Terrorism Centre (ECTC)
	Legal Expert
europa.eu	European Counter Terrorism Centre (ECTC)
	D.F. Expert
	Legal Expert

	7	Digital Forensic Software companies						
		Name of organization	**Geographical reach**	**Town**	**Country**	**Contact Person**	**e-mail address**	**To be invited to Project workshops**
F1	87	Kasperky Lab	International			Anastasiya Kazakova	Anastasiya.Kazakova@kaspersky.com	
F2	88	Microsoft	International			Hasan Ali, Senior Attorney	hasanali@microsoft.com	
G1	89	ICT Unit MoJ	International	Madrid	Spain	Jose Merli Gisbert	josefrancisco.merli@mju.es	Yes

	Back to cheklist
To be involved in other Project initiatives	**Note**
	CEO Projects Coordinator
	Law Enforcement & National Security (LENS) – Policy & Strategy
Yes	J.Merli is involved in e-Codex , e-Evidence projects as well

	8	Digital Forensic Hardware producers						
		Name of organization	**Geographical reach**	**Town**	**Country**	**Contact Person**	**e-mail address**	**To be invited to Project workshops**
Y3	90	Magnet Forensics		New York	USA	Jessica Hyde	jessica.hyde@magnetforensics.com	
Y4	91	MSAB		Stockolm	Sweden	Martin Westman	Martin.Westman@msab.com	
Y5	92	Netresec		Orsundsbro	Sweden	Erik Hjemvik	erik.hjelmvik@netresec.com	
Y6	93	AccessData		Lindon (UT)	USA	Theo Sbarounis	tsbarounis@accessdata.com	
Y7	94	Cellebrite		Petah Tiqwa	Israel	Danny Rosenzweig	Danny.Rosenzweig@cellebrite.com	
Z12	95	Magnet Forensics				Hans Henseler	Hans.Henseler@magnetforensics.com	

	Back to cheklist
To be involved in other Project initiatives	**Note**
	Director of forensics
	Director Digital Evidence Review

	9	Internet Service Providers / Tech companies						
		Name of organization	**Geographical reach**	**Town**	**Country**	**Contact Person**	**e-mail address**	**To be invited to Project workshops**
E1	96	Vodafone	International	Brussels	Belgium	Laure Wagner	laure.wagener@vodafone.com	Yes
E2	97	Microsoft	International	Brussels	Belgium	Lani Cossette	lanic@microsoft.com	Yes
E3	98	BSA - The Software Alliance	International	Brussels	Belgium	Alexander Whalen	alexw@bsa.org	Yes
G1	99	ISDEFE Spanish company providing service to Public administration	International	Madrid	Spain	Jose Manuel Martinez Jimenez	jmmartinez@isdefe.es	Yes
C1	100	ISPA	National	Vienna	Austria	Dr. Maximilain Schubert	maximilian.schubert@ispa.at	Yes
C2	101	VAT	National	Vienna	Austria	Mag. Florian Schnurer	office@vat.at	Yes
C3	102	Telekom Austria	National	Vienna	Austria	Marieluise Gregory	Marielouise.Gregory@a1telekom.at	Yes
D1	103	IT.NRW	Regional	Düsseldorf	Germany	Tim-Marco Nowosadtko	Tim-Marco.Nowosadtko@it.nrw.de	Yes
X1	104	Austrian Federal Computing Centre		Vienna	Austria	Robert Behr	robert.behr@brz.gv.at	
X2	105	Austrian Federal Computing Centre		Vienna	Austria	Mathias Maurer	mathias.maurer@brz.gv.at	
X3	106	Austrian Federal Computing Centre		Vienna	Austria	Bernhard Rieder	Bernhard.Rieder@brz.gv.at	
X4	107	Austrian Federal Computing Centre		Vienna	Austria	Stephan Spindler	Stephan.Spindler@brz.gv.at	

	Back to cheklist
To be involved in other Project initiatives	**Note**
Yes	
Yes	
Yes	
Yes	Involved in technical developemnts in e-codex, e-evidence as well
Yes	https://www.ispa.at/wissenspool/broschueren/team.html
Yes	https://www.ispa.at/wissenspool/broschueren/team.html
Yes	Head of legal department at Austria's incumbent
Yes	e-Codex; EXEC

	10	Forensic examiners						
		Name of organization	**Geographical reach**	**Town**	**Country**	**Contact Person**	**e-mail address**	**To be invited to Project workshops**
A1	108	Bulgarian Association of Forensics Experts	National	Sofia	Bulgaria		office@expert-bg.com	Yes
Y1	109	NFI Netherlands Forensic Institute		The Hague	The Netherlands	Hram van Beek	harm.van.beek@nfi.minvenj.nl, harm@holmes.nl	
Z18	110	Reality Net		Genoa	Italy	Francesco Picasso	francesco.picasso@realitynet.it	

	Back to cheklist
To be involved in other Project initiatives	**Note**
Yes	
	D.F. Expert

	11	Policy makers at national level						
		Name of organization	**Geographical reach**	**Town**	**Country**	**Contact Person**	**e-mail address**	**To be invited to Project workshops**
G1	111	REPER Councelor of Justice	International	Brussels	Belgium	Joaquin Silguero Estagnan		Yes
B1	112	Ministry of Justice / Direção-Geral de Política de Justiça (DGPJ)	National	Lisbon	Portugal	Luísa Pacheco	maria.l.pacheco@dgpj.mj.pt	Yes
B2	113	Ministry of Justice / Direção-Geral de Política de Justiça (DGPJ)	National	Lisbon	Portugal	António Folgado	antonio.j.folgado@dgpj.mj.pt	Yes
C1	114	ÖVP	National	Vienna	Austria	Eva-Maria Himmelbauer	eva-maria.himmelbauer@parlament.gv.at	Yes
C2	115	FPÖ	National	Vienna	Austria	Christian Hafenecker	christian.hafenecker@parlament.gv.at	Yes
C3	116	SPÖ	National	Vienna	Austria	Philipp Kucher	philip.kucher@parlament.gv.at	Yes
C4	117	FPÖ	National	Vienna	Austria	Gerhard Deimek	gerhard.deimek@fpoe.at	Yes
C5	118	NEOS	National	Vienna	Austria	Dr. Nikolaus Scherak	nikolaus.scherak@parlament.gv.at	Yes

	Back to cheklist
To be involved in other Project initiatives	**Note**
Yes	
Yes	
Yes	
Yes	Member of Parliament's Committe on Digitalisation and Innovation
Yes	https://www.parlament.gv.at/WWER/PAD_78586/index.shtml
Yes	https://www.parlament.gv.at/WWER/PAD_83113/index.shtml
Yes	https://www.parlament.gv.at/WWER/PAD_51557/index.shtml
Yes	Head of Parliament's Committe on Human Rights, https://www.parlament.gv.at/WWER/PAD_83125/index.shtml

	12	Ministries of Justice of UE MS						
		Name of organization	**Geographical reach**	**Town**	**Country**	**Contact Person**	**e-mail address**	**To be invited to Project workshops**
D1	119	Ministry of Justice, North Rhine-Westphalia/GER	Local	Düsseldorf	GER	Dr. Sebastian Trautmann	sebastian.trautmann@jm.nrw.de	Yes
B1	120	Ministry of Justice	National	Lisbon	Portugal	Manuel Magriço	manuel.magrico@mj.gov.pt	Yes
C1	121	Federal Ministry of Constitutional Affairs, Reforms, Deregulation and Justice	National	Vienna	Austria	Dr. Josef Moser		Yes
F1	122	Ministry of Justice	National		Ireland	Brendan EIFFE	Bjeiffe@justice.ie	
F2	123	Ministry of Justice	National	Reykjavik	Iceland	Hinrika Sandra	hinrika.s.ingimundardottir@dmr.is	
G1	124	e-Justice Delegate MoJ	Regional	Madrid	Spain	Ana E. Sanchez Garcia	anaesther.sanchez@mjusticia.es	Yes
X5	125	Federal Ministry of Constitutional Affairs, Reforms, Deregulation and Justice		Vienna	Austria	Thomas Gottwald	thomas.gottwald@bmvrdj.gv.at	
X6	126	Federal Ministry of Constitutional Affairs, Reforms, Deregulation and Justice		Vienna	Austria	Judith Herrnfeld	Judith.Herrnfeld@bmvrdj.gv.at	
Z7	127	Ministry of Justice - The Netherlands			The Netherlands	Huub Moelker	h.moelker@justid.nl	
Z11	128	Ministry of Justice - Estonia			Estonia	Elen Kraavik	elen.kraavik@just.ee	
Z13	129	Ministry of Justice - Estonia			Estonia	Julia Antonova	julia.antonova@just.ee	

Z14	130	Ministry of Justice - Bulgaria			Bulgaria	Ivan Nurkov	i_nurkov@justice.government.bg	
Z15	131	Ministry of Justice - Bulgaria			Bulgaria	Aleksander Dimitrov	a_dimitrov@justice.government.bg; gsm.sasho@gmail.com	
Q2	132	Ministry of Justice - Italy			Italy	Fabrizia Bemer	fabrizia.bemer@giustizia.it	
Q3	133	Belgian Federal Public Service Justice			Belgium	Nathalie Cloosen	Nathalie.Cloosen@just.fgov.be	
Q4	134	Belgian Federal Public Service Justice			Belgium	Luc De Houwer	luc.dehouwer@just.fgov.be	

	Back to cheklist
To be involved in other Project initiatives	**Note**
Yes	e-codex; EXEC
Yes	
Yes	No e-mail adress provided, contact via
	Head of the Mutual Legal Assistance Section
	Senior Legal Advisor, in charge of hand
Yes	
	Business Consultant
	Adviser in Criminal Law and Data Protection

	IT expert from e-Justice and Registers Directorate, representative in the e-Law WP at the EC
	IT expert from e-Justice and Registers Directorate, representative in the e-Law WP at the EC
	Officer at the international judicial cooperation office on the EIO

	14	Policy makers at European level						
		Name of organization	**Geographical reach**	**Town**	**Country**	**Contact Person**	**e-mail address**	**To be invited to Project workshops**
E1	135	MEP Sophie in 't Veld	Regional	Brussels	Belgium		sophie.intveld@europarl.europa.eu	Yes
E2	136	MEP Birgit Sippel	Regional	Brussels	Belgium		birgit.sippel@europarl.europa.eu	Yes
E3	137	MEP Daniel Dalton	Regional	Brussels	Belgium		daniel.dalton@europarl.europa.eu	Yes
E4	138	MEP Nuno Melo	Regional	Brussels	Belgium		nuno.melo@europarl.europa.eu	No
E5	139	MEP Pavel Svoboda	Regional	Brussels	Belgium		pavel.svoboda@europarl.europa.eu	No
E6	140	MEP Juan Fernando Lopez Aguilar	Regional	Brussels	Belgium		juanfernando.lopezaguilar-office@europarl.europa.eu	No
E7	141	MEP Axel Voss	Regional	Brussels	Belgium		Axel.voss@europarl.europa.eu	No
E8	142	MEP Frank Engel	Regional	Brussels	Belgium		frank.engel@europarl.europa.eu	No
E9	143	Council of the EU	Regional	Brussels	Belgium	Alain Pilette	Alain.Pilette@consilium.europa.eu	No
Q1	144	European Parliament	Regional			Sarah-Maria Hartmann	sarah-maria.hartmann@europarl.europa.eu	
Q2	145	Council of the EU - General Secretariat	Regional			Filipa Melo Antunes	filipa.melo-antunes@consilium.europa.eu	

Q3	146	Council of the EU - General Secretariat	Regional			Monika Kopcheva	monika.kopcheva@consilium.europa.eu	
Q4	147	European Commission	Regional			Nada Milisavljevic	Nada.MILISAVLJEVIC@ec.europa.eu	
Q5	148	European Commission	Regional			Karl Linderborg	karl.linderborg@ec.europa.eu	
Z5	149	European Commission	Regional			Djamila Ben-Miloud	djamila.ben-miloud@ext.ec.europa.eu	
Z6	150	European Commission	Regional			Cristian Nicolau	cristian.nicolau@ec.europa.eu	
G9	151	Council of Europe	Regional	Strasbourg	France	SEGER Alexander	Alexander.SEGER@coe.int	Yes
F1	152	Council of Europe	Regional	Strasbourg	France	Peter Kimpian	Peter.KIMPIAN@coe.int	
Q6	153	DG Justice and Consumers				Toma Milieskaite	Toma.MILIESKAITE@ec.europa.eu	
Q7	154	DG Justice and Consumers				Michael Palmer	michael.palmer@ec.europa.eu	
Q8	155	European Parliament - LIBE Committee				Anže Erbežnik	anze.erbeznik@europarl.europa.eu	

	Back to cheklist
To be involved in other Project initiatives	**Note**
Yes	
Yes	
Yes	
Yes	
Yes	
Yes	
Yes	
Yes	
Yes	
	MEPs Birgit SIPPEL assistant
	Political Administrator

	Political Administrator - Cyber Issues, General Secretariat of the Council of the EU
	IT Consultant, DG Justice
	Head of Unit, IT and document management, DG Justice
	Programme Advisor, Data Protection Unit
	Legal officer, DG JUST, Procedural Criminal Law
	DG JUST, Procedural Criminal Law
	Administrator, Committee on Civil Liberties, Justice and Home Affairs

	15	Other on-going EU Projects						
		Name of organization	**Geographical reach**	**Town**	**Country**	**Contact Person**	**e-mail address**	**To be invited to Project workshops**
B1	156	High Judicial Council	National	Lisbon	Portugal	Ruben Juvandes	rubenjuvandes@gmail.com	Yes
B2	157	Prosecutor General's Office	National	Lisbon	Portugal	Rui Batista	rui.batista@pgr.pt	Yes
B3	158	Institute of Registration and Notary Affairs	National	Lisbon	Portugal	Sofia Carvalho	sofia.c.carvalho@irn.mj.pt	Yes
E1	159	Judicial Cooperation in Criminal Matters and Electronic IT Data in the EU (JUD-IT)	Regional	Brussels	Belgium	Marco Stefan (Center for European Policy Studies)	marco.stefan@ceps.eu	Yes

	Back to cheklist
To be involved in other Project initiatives	**Note**
Yes	Participate in: - Find an Expert project - ECLI.PT – Sharing Portuguese Case Law in e-Justice Portal project - e-CODEX Plus: European Small Claims; European Payment Order (EIO) project
Yes	Participate in Find an Expert project
Yes	Connecting Portuguese SIRCOM to BRIS
Yes	

16	Legal and forensic associations and networks						
	Name of organization	**Geographical reach**	**Town**	**Country**	**Contact Person**	**e-mail address**	**To be invited to Project workshops**
160	Audit data cybersecurity	Regional		EU	Philippe Vynckier	pvynckier@gmail.com	

To be involved in other Project initiatives

	17	Research bodies, associations and networks								Back to cheklist
		Name of organization	Geographical reach	Town	Country	Contact Person	e-mail address	To be invited to Project workshops	To be involved in other Project initiatives	Note
A2	161	Leaders in Security (LSEC)	International	Leuven	Belgium	Ulrich Seldeslachts	ulrich@anakyn.be	Yes	Yes	
A3	162	Cyber Security Centre, University of Warwick	International	Coventry	United Kingdom	Bil Hallaq	<bh@warwick.ac.uk>	Yes	Yes	
A4	163	Centrum Badań Problemów Prawnych i Ekonomicznych Komunikacji Elektronicznej	International	Wrocław	Poland	Damian Klimas	damian.klimas@uwr.edu.pl	Yes	Yes	
C1	164	Ludwig Boltzmann Institut für Menschenrechte	International	Vienna	Austria	Prof. Dr. Hannes Tretter	hannes.tretter@univie.ac.at	Yes	Yes	http://bim.lbg.ac.at/
A1	165	Research Forensics Science Institute of Bulgaria	National	Sofia	Bulgaria		int.27@mvr.bg	Yes	Yes	
B1	166	Polytechnic of Leiria / Center for Research in Informatics and Communications (CIIC)	National	Leiria	Portugal	Miguel Frade	miguel.frade@ipleiria.pt	Yes	Yes	The Polytechnic of Leiria is a higher education institution committed to education and research. The research carried out at IPLeiria and CIIC in the forensic area covers the development of projects within advanced training courses and the development of methodologies and procedures that lead to the continuous improvement of digital forensics (http://ciic.ipleiria.pt/index.php/en/)
F1	167	The Norwegian Police University College/ Arsforensica NTNU	National		Norway	Jul Fredrik Kaltenborn	Jul.Fredrik.Kaltenborn@phs.no			Assistant Professor/PhD-fellow highly interested to be involved in the project
J1	168	Polytechnic Institute of Beja		Beja	Portugal	Rui Miguel Soares Silva				Portugal, Course Coordinator of the Master in Computer Science Security Engineering, at IPBeja, and Lab Coordinator of the UbiNET - Computer Science Security and Cybercrime (https://ubinet.ipbeja.pt/rui/index_en.html
J2	169	Polytechnic Institute of Beja		Beja	Portugal	Mário Jorge Candeias				assistant at the MSc in Computer Security Engineering and Invited Researcher at UbiNET - Computer Science Security and Cybercrime (https://ubinet.ipbeja.pt/index_en.html)
Y2	170	UNIL University of Lasaunne		Lausanne	Switzerland	Eoghan Casey	eoghan.casey@unil.ch			
Z10	171	Fraunhofer ESK				Mathias Leibiger	mathias.leibiger@esk.fraunhofer.de			Group Manager Access & Inhouse Networks
Q1	172	Centre for European Policy Studies - Belgium				Sergio Carrera	sergio.carrera@ceps.eu			CEPS
Z8	173	European Cybercrime Training and Education Group (ECTEG)				Ray Genoe	ray.genoe@ucd.ie			Chair

	18	Actors involved in the field of human rights						
		Name of organization	**Geographical reach**	**Town**	**Country**	**Contact Person**	**e-mail address**	**To be invited to Project workshops**
C1	174	NOYB	International	Vienna	Austria	Max Schrems	info@noyb.eu	Yes
C2	175	Epicenter Works	International	Vienna	Austria	Dr. Christof Tschohl	christof.tschohl@univie.ac.at	Yes
E1	176	Fair Trials	International	Brussels	Belgium	Ralph Bunch	Ralph.bunche@fairtrials.net	Yes
F1	177	Electronic Frontier Foundation	International		USA	Katitza Rodriguez	Katitza@eff.org	
E2	178	European Digital Rights (EDRi)	Regiona	Brussels	Belgium	Maryant Fernandez Perez	maryant.fernandez-perez@edri.org	Yes

	Back to cheklist
To be involved in other Project initiatives	**Note**
Yes	
Yes	https://epicenter.works/
Yes	
	International Rights Director
Yes	

	19	Scientific and technical journals and web sites						
		Name of organization	**Geographical reach**	**Town**	**Country**	**Contact Person**	**e-mail address**	**To be invited to Project workshops**
C1	179	JusIt	International	Vienna	Austria	Prof. Dr. Dietmar Jahnel	Dietmar.Jahnel@sbg.ac.at	Yes
C2	180	ZIIR	International	Vienna	Austria	Dr. Thomas Hoehne	office@voe.at	Yes

	Back to cheklist
To be involved in other Project initiatives	**Note**
Yes	https://lesen.lexisnexis.at/zs/jusit/index.html
Yes	https://www.verlagoesterreich.at/zeitschrift-fuer-informationsrecht-2306-4900

	20	The media						
		Name of organization	**Geographical reach**	**Town**	**Country**	**Contact Person**	**e-mail address**	**To be invited to Project workshops**
C1	181	ORF	International	Vienna	Austria			Yes

	Back to cheklist
To be involved in other Project initiatives	**Note**
Yes	www.orf.at