



## D3.2 DEVELOPMENT OF A DECISION-MAKING-MECHANISM

<b>Grant Agreement:</b>	833635
<b>Project Acronym:</b>	ROXANNE
<b>Project Title:</b>	Real time network, text, and speaker analytics for combating organised crime
<b>Call ID:</b>	H2020-SU-SEC-2018-2019-2020,
<b>Call name:</b>	Technologies to enhance the fight against crime and terrorism
<b>Revision:</b>	V1.0
<b>Date:</b>	18 January 2020
<b>Due date:</b>	01 October 2020 (Delay to 1 January 2021 agreed)
<b>Deliverable lead:</b>	TRI
<b>Work package:</b>	WP3
<b>Type of action:</b>	RIA

## Disclaimer

The information, documentation and figures available in this deliverable are written by the “ROXANNE - ” Real time network, text, and speaker analytics for combating organised crime” project’s consortium under EC grant agreement 8833635 and do not necessarily reflect the views of the European Commission.

The European Commission is not liable for any use that may be made of the information contained herein.

Copyright notice

© 2019 - 2022 ROXANNE Consortium

Project co-funded by the European Commission within the H2020 Programme (2014-2020)		
Nature of deliverable:		PU
Dissemination Level		
<b>PU</b>	Public	<input checked="" type="checkbox"/>
<b>CO</b>	Confidential, only for members of the consortium (including the Commission Services)	<input type="checkbox"/>
<b>EU-RES</b>	Classified Information: RESTREINT UE (Commission Decision 2015/444/EC)	<input type="checkbox"/>
* R: Document, report (excluding the periodic and final reports) DEM: Demonstrator, pilot, prototype, plan designs DEC: Websites, patents filing, press & media actions, videos, etc. OTHER: Software, technical diagram, etc.		

## Revision history

Revision	Edition date	Author	Modified Sections / Pages	Comments
V0.1	17/12/2020	Joshua Hughes (TRI); Shivam Garg (CAPGEMINNI); Stela Lipcan (INTERPOL); Theoni Spathi (KEMEA); Neil Toffa (AIRBUS).	All	Original draft
V0.2	18/12/2020	Costas Kalogiros (AEGIS)	All	Review
V0.3	21/12/2020	Joshua Hughes (TRI)	All	Edits
V0.4	28/12/2020	Georgia Melenikou (KEMEA)	All	Review
V0.5	29/12/2020	Joshua Hughes (TRI)	All	Edits
V0.6	17/1/2021	Petr Motlicek (IDIAP)	All	Review
V1.0	18/1/2021	Joshua Hughes (TRI)	All	Final edits.

## Executive summary

This document explains the intended nature of human decision-making when using the ROXANNE platform. It explains ethical, societal, and legal risks associated with automated decision-making and shows how they can be avoided through maintaining critical human engagement with the results generated by the ROXANNE platform. This engagement is facilitated by asking end-users to answer questions about their intended use of the platform, and how they understand the results. Mock-ups of the decision-making mechanism in electronic form are also provided, as there are details of Data Protection Authorities who we will send the decision-making mechanism in order to gain feedback.

## Table of contents

Disclaimer	2
Executive summary	4
Table of contents	5
1. Introduction	6
1.1. Background	6
1.2. Purpose and scope	6
1.3. Document structure	6
2. The human-centred approach in ROXANNE	7
2.1. Avoiding risks in automated decision-making	7
2.2. Focussing on decision-support not decision-making	9
2.3. Legal ‘neutrality’ and adaptability for end-users	10
3. The decision-making mechanism	11
3.1. Intended use	11
3.2. Structure	11
3.3. Decision-making at the procurement stage	12
3.4. Decision-making at the beginning of a new case	15
3.5. Decision-making when using new data	19
3.6. Decision-making after data has been analysed	22
4. The decision-making mechanism in electronic form	23
4.1. Technical and design specification	23
4.2. Mock-up of the decision-making mechanism	24
5. Sending Decision-making mechanism to Data Protection authorities	27
5.1. Authorities chosen	27
5.2. Opportunity for feedback/validation	29
6. Conclusion	29

## 1. Introduction

### 1.1. Background

This deliverable D3.2 responds to the following task:

*‘The partners will create a framework, based on the forgoing tasks that will help stakeholders determine whether they comply with ethical principles, social values, fundamental rights and relevant legislation. The partners will send the decision-making mechanism to Data Protection Officer organisations (i.e. Data Protection Authorities) in project member countries.’*

This deliverable builds upon the work of D3.1 (Initial report on compliance with ethical principles). That deliverable highlighted ethical, societal, and legal issues and risks that could be raised in the development and use of the proposed ROXANNE platform. The present work uses those risks and issues as a starting point to highlight points that LEA officers should consider when using the ROXANNE platform to ensure that their use is in compliance with the ethical, societal, and legal standards that were previously analysed.

The decision-making tools discussed below are intended to be used by Law Enforcement Agencies (LEAs) both prior to, and whilst, using the proposed ROXANNE platform. Therefore, ROXANNE partners want the tools to be appropriate for, and fit within, the context of LEA investigations. To this end, partners working on this decision-making mechanism met with LEA partners and presented the approach and proposed structure of the decision-making tools to them. Options for how the tools could be employed, and how they might work best with the ROXANNE platform were discussed, and the results of this consultation are included in the analysis provided below.

### 1.2. Purpose and scope

The purpose of this deliverable is to describe how the use of the proposed ROXANNE platform fits within the intended human-machine relationship including LEA officers.

Its scope is to present the position of the ROXANNE consortium with regard to keeping a human being in control of the system who takes all decisions about how the platform is used and how its results are understood and implemented. To facilitate this, four sets of questions that can be considered by LEA officers to ensure compliance with ethical, societal, and legal standards are presented; it is intended that these questions will be adapted to the specific needs of each LEA who employs the proposed ROXANNE platform. How these questions are integrated with the ROXANNE platform is explained and displayed through screenshots of the questions in electronic form.

### 1.3. Document structure

Following this brief introduction, Section 2 explains risks of automated decision-making and how the ROXANNE project intends to facilitate a human-centred approach to decision making with the proposed ROXANNE platform. Section 3 provides the four-stage decision-making mechanism that can be used by LEAs to ensure compliance with ethical, societal, and legal standards. Section 4 shows how the decision-making mechanism will be presented in an electronic version, and also displays mock-ups of what this electronic version looks like. Section 5 details how an edited version of this document will be sent to Data Protection Authorities for feedback.

## 2. The human-centred approach in ROXANNE

### 2.1. Avoiding risks in automated decision-making

The ROXANNE consortium is acutely aware of the risks of automated decision-making where it results in significant effects on people,<sup>1</sup> and especially in the law enforcement domain.<sup>2</sup> As mentioned in D3.1 (Initial report on compliance with ethical principles), there are significant ethical, societal, and legal issues where human beings delegate their decision-making to machines and allow those decisions to affect others.

Automated decision-making can create ethical and societal issues that can affect both the people who are affected by the decisions, and those who delegate them. As algorithms are not inherently objective, but are impacted by the effects of choices taken during their development, they cannot produce results that have completely equal effects.<sup>3</sup> Whilst human beings can also make unequal decisions, they are more often easily fixable.<sup>4</sup> Automated decision-making can entrench the effects of structural issues in society, whilst presenting a veneer of objectivity.<sup>5</sup> Thus, there is a need to avoid automated decision-making due to the negative effects it can have on the people whom technologies are used on.

Retaining the critical engagement of human beings using technologies is also key to avoiding issues that could be caused for the end-users. D3.1 (Initial report on compliance with ethical principles) noted that end-users can be alienated from their work when it is mediated through machines,<sup>6</sup> and that this could lead to a loss of intuition for LEA officers, alongside a risk of atrophying moral decision-making skills,<sup>7</sup> and potential impacts on the role of LEA officers as ‘*societal moral agents*’.<sup>8</sup>

In terms of legal effects, automated decision-making can result in increased efficiencies and resource saving, but also presents clear risks of removing the ability for people to choose and can also lock people into specific categories that could be subject to discrimination.<sup>9</sup> Thus, in both the General Data Protection Regulation (GDPR) and the Law Enforcement Directive (LED), there is a general prohibition on the use of automated decision-making where this creates legal, or similarly significant effects.<sup>10</sup>

Solely automated decision-making is where decisions are made using technological means without human involvement.<sup>11</sup> Automation happens where a person delegates the mental labour of making a decision to a machine.<sup>12</sup> But, automated decision-making can still happen where there is only ‘*token*’ human oversight; for

<sup>1</sup> Art.22, European Parliament and Council, Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, OJ L 119, Vol.59, 4 May 2016 (General Data Protection Regulation, hereafter: GDPR)

<sup>2</sup> Art.11, European Parliament and Council, Directive (EU) 2016/680 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, OJ L 119/89, Vol.59, 4 May 2016 (Law Enforcement Directive, hereafter: LED)

<sup>3</sup> See Eubanks, Virginia, *Automating Inequality*, St Martins Press, New York, 2018, and Benjamin, Ruha, *Race Against Technology*, Polity Press, 2019

<sup>4</sup> Eubanks, Virginia, *Automating Inequality*, St Martins Press, New York, 2018, Chapter 4.

<sup>5</sup> Benjamin, Ruha, *Race Against Technology*, Polity Press, 2019, Chapter 1.

<sup>6</sup> Marx, Karl (trans Martin Nicolaus), *Grundrisse*, Penguin, St Ives, 1993, p.701; Virilio, Paul (trans Chris Turner), *The Information Bomb*, Verso, London 2000, p.123.

<sup>7</sup> Brownsword, Roger, “In the year 2061: from law to technological management” *Law, Innovation and Technology*, Vol.7, No.1, 2015, pp.1-51, 35.

<sup>8</sup> See, for example, Dirix Astrid, Jan Van den Bulck, and Stephan Parmentier, “The Police as Societal Moral Agents: “Procedural Justice” and the Analysis of Police Fiction” *Journal of Broadcast and Electronic Media*, Vol.56, No.1, 2012, pp.38-54

<sup>9</sup> Article 29 Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679. 17/EN, WP251.01, Revised and Adopted on 6 February 2018, pp.5-6. (Hereafter: Art.29WP Guidelines) Available at: <https://idpc.org/mt/wp-content/uploads/2020/08/EDPB-automated-decision-making-under-GDPR.pdf>

<sup>10</sup> Art.22, GDPR Art.11, LED.

<sup>11</sup> Art.29WP Guidelines, p.8.

<sup>12</sup> Pyke, Magnus, *Automation: Its purpose and future*, Scientific Book Club, London, 1946, p.38.

example, a situation where someone simply pushes a button to confirm and enact a machine result would be seen as a situation of solely automated decision-making.<sup>13</sup> Indeed, for decision-making not to be ‘solely automated’, a human being must consider ‘*all the relevant data*’.<sup>14</sup>

With the proposed ROXANNE platform, the intention has always been to maintain meaningful human involvement by building the platform in such a way that human beings must take all decisions based on the outputs/results generated. In order to facilitate this, the ROXANNE partners have developed the below decision-making mechanism for human beings to use to assist them in coming to decisions about data use and how results should be understood. This is in the form of questions that facilitate critical engagement by end-users in order to fully consider all relevant data. This should mean that the ultimate decision about how the results of the ROXANNE analysis are comprehended and implemented in LEA investigations are made by a person and, therefore, are not solely automated.<sup>15</sup> The tools below are for decision-support, not decision-making on behalf of the users.

With regard to human involvement in decision-making, the ROXANNE partners are also conscious of the risks of automation bias. This is where human beings begin to trust the results of machine analysis more than themselves.<sup>16</sup> The ultimate effect of this can be that, where a human does not apply their own critical engagement to the results of a tool, the human is, in-effect, a by-stander, and the machine is acting autonomously for all intents and purposes.<sup>17</sup> Automation bias is different from the ‘token’ human involvement mentioned above: ‘token’ human involvement can be a design choice, whereas automation bias is choice made by end-users. However, the effects are the same with both resulting in a lack of critical engagement by end-users.

A significant amount of literature on avoiding automation bias has been written in relation to autonomous weapon systems. Sharkey suggests that the ideal level of human control over a machine that has effects on humans should be where a human being can deliberate on the results of machine analysis and place them within the context provided by situational awareness of the circumstances at hand (i.e. consider all the relevant data).<sup>18</sup> Consequently, in order to facilitate critical engagement with the issues applicable to the use of ROXANNE, and to avoid automation bias, the ROXANNE partners opted to develop questions for LEA officers to answer during their use of the proposed ROXANNE platform.

This has two key benefits. First, it provides an opportunities for LEA officers to: examine the crucial ethical, societal, and legal issues related to their data use; ensure that they understand the meaning of the results of the ROXANNE platform before acting upon them; evidence and attest that their actions are in compliance with applicable legal and ethical standards and, where relevant, the terms of any warrants that the LEAs are operating under. Second, it is an obvious point at which to implement accountability measures by logging the users of the ROXANNE platform, their reasons for using it, and the outcomes which they take forward into investigations.

In terms of the examination of ethical, societal, and legal issues, and attesting to compliance to the relevant standards for these issues, it is important that LEA officers understand these issues prior to commencing with data processing. This is because there can be ethical, societal, and legal risks associated with the data processing using ROXANNE in addition to those associated with collecting it. For example, there could be a legitimate violation of privacy in collecting telephone intercepts from a suspect in a criminal case; but, analysing their data can be seen as a distinct activity where the legitimacy of a further privacy violation should be assessed separately. Therefore, it is important that compliance risks are assessed before the analysis takes place. Further, LEAs must ensure that where they are acting under a warrant that they comply with the terms of that warrant. One of the ROXANNE LEA partners noted that such an assessment could facilitate their

<sup>13</sup> Art.29WP Guidelines, p.21.

<sup>14</sup> Art.29WP Guidelines, p.21.

<sup>15</sup> See Bundesgerichtsof, *Urteil vom 28.1.2014*, Para.34.

<sup>16</sup> Skitka, Linda J., Kathleen L. Mosier and Mark Burdick, 'Does Automation Bias Decision-Making?' (1999) 51 *International Journal of Human-Computer Studies*, pp.991-1006.

<sup>17</sup> So-called ‘Functional Autonomy’ in Roff, Heather M., 'The Forest For The Trees: Autonomous Weapons And “Autonomy” In Weapons Systems' [2016] Unpublished Essay.

<sup>18</sup> Sharkey, Noel, “Staying in the loop: human supervisory control of weapons”, in Nehal Bhuta and others (eds.), *Autonomous Weapons Systems*, CUP, Cambridge, 2016, pp.34-35.



compliance with the conditions of a warrant if, for example, it required investigators to demonstrate that an infringement on the privacy of a suspect is the last resort, and their reasoning could be included, and recorded, in their responses to decision-making questions.

Having investigators demonstrate that they understand the results of the ROXANNE platform is beneficial not only for compliance with ethical, societal, and legal standards, but also for operational reasons. The proposed ROXANNE platform will integrate several tools and functions that already operate in complicated ways, and having them work together in a processing chain could add layers of complexity that hamper end-users understanding the results and how they were generated.

There are different factors that can better facilitate the understanding that end-users have for results. First, of course, are technical approaches that enable end-users to comprehend the results more easily in the way they are presented and explained to end-users. This is an area of continuing discussion with technical partners; requirements on this topic arose in D3.1 (Initial report on compliance with ethical principles), and their fulfilment will be reported in D3.4 (Final report on compliance with ethical principles). Second, is prompting users to engage with the results and critically assess their meaning. Having users engage with the context in which both the original data were gathered, and the results are generated can lead to greater understanding. For example, data analysis results could suggest a criminal suspect has met with accomplices, but an investigator might know that the suspect was in prison at the time and so cannot have met accomplices. Thus, interpreting the results of the data analysis in context is needed.

To enhance the understanding of the ethical and legal risks when analysing ROXANNE results, it is recommended to foresee the need for the users of the platform to complete training on this topic. This can allow investigators to better understand the relevant issues, and allow them to fully engage with them when they use the ROXANNE platform. The training modules should explain how the platform functions, what its technical limitations are, and how the users should use it. Thus, users should clearly understand that the results do not accurately reflect reality and the platform may highlight patterns without being able to explain them. The training should underline that decisions stay with the investigators using the platform and they should be made only after having critically evaluated the results provided by the platform. Hence, the officers using the platform should learn to interpret ROXANNE results and to accurately present them to judges and juries. The training should also raise the users' awareness of legal requirements linked to their use such as ethical, data protection and fundamental rights. Users should take into consideration all these legal aspects when using the platform and evaluating the potential impact of their decisions.

## 2.2. Focussing on decision-support not decision-making

Earlier, the risks associated with end-users being 'alienated' from their work were noted along with the need to retain the critical engagement of investigators when using the ROXANNE platform. As such, it is important to clarify that references to a 'decision-making mechanism', in the title of this deliverable and the description of the task it fulfils, this should not be read to indicate that decisions are taken on behalf of users. Rather, the series of questions offered below are a mechanism for facilitating decision-making, and, in that sense, are tools to support human decision-making, rather than allow decisions to be delegated to the ROXANNE platform.

The questions below can be seen as decision-support tools though prompting end-users to consider various topics that are relevant to the use of ROXANNE. Indeed, the purpose is to follow a human-centred approach to using the ROXANNE platform and keep the 'human-in-the-loop'. The loop paradigm for understanding human-machine relationships comes from literature on autonomous weapon systems,<sup>19</sup> and can be adapted for the context of a data analysis platform: a human 'in-the-loop' analyses results from the machine and takes decisions themselves; a human 'on-the-loop' would observe decisions by the machine and intervene where necessary; a human 'out-of-the-loop' would allow the machine to make decision for them. In the case of ROXANNE, the consortium partners have only ever intended for the platform to be used with a human 'in-the-loop'; it is not being built to allow for uses where a human could be 'on-' or 'off-the-loop'.

<sup>19</sup> Human Rights Watch, *Losing Humanity*, Human Rights Watch and the International Human Rights Clinic, Cambridge MA, 2012, p.2.

We can also consider other paradigms for understanding ROXANNE in order to further demonstrate that the proposed platform is firmly under human control. The ‘Levels of Autonomy’ paradigm describes how the technological capabilities of machines can be seen along a spectrum from inert, to automated, to semi-autonomous, and fully-autonomous systems.<sup>20</sup> The proposed ROXANNE platform would remain in the inert category as, despite containing very advanced computing, it will not be capable of functioning without a human being directing it.

Further, the intended tasks of the ROXANNE platform are purely data analysis, it would not be possible for the platform itself to have any material effect on the world (any effects arising from the use of the ROXANNE platform would need to be enacted by the human beings using it).<sup>21</sup> Consequently, it is not possible to view the platform as being used for the delegation of decision-making. The proposed ROXANNE platform should, according to the most commonly used paradigms, be seen as an inert system carrying out data analysis tasks only at the direction of a user who is ‘in-the-loop’ and makes all decisions regarding the results of that analysis and how it should be used.

### 2.3. Legal ‘neutrality’ and adaptability for end-users

Since the beginning of the project, LEAs have been asked to report their needs and requirements for the ROXANNE platform through specific questionnaires which were reviewed and complemented using the feedback sessions of the field tests and the regular LEAs meetings. From the initial end user requirements survey, which was distributed within the ROXANNE project, stakeholder board LEA members and through INTERPOL’s global law enforcement network (194 member countries), 121 responses from 40 countries had been gathered, mainly from police services, academia and anti-terrorism units. Those were mainly focused on the current data sources, data types, current technologies, their main obstacles and challenges as well as their desired features and options for the platform. LEAs did not share any specific input around the decision-making mechanism, rather they shared their thoughts on the issues and obstacles which prevent them from making the most out of each data type, from not using web/social media data to its full potential, as well as with respect to data handling and analysis which could prevent criminal investigations to succeed, underlining legal constraints as a really important topic. As the questionnaires did not request specific input regarding the decision-making mechanism, a meeting was held with ROXANNE LEA partners to discuss a proposed decision-making mechanism and how it could work best with current LEA approaches to investigations.

In addition to the end-user surveys, a supplementary legal requirements survey brought forward the need for legal solutions neither specific to particular types of investigations or organisations nor focussed toward a particular legal regime, due to the fact that pre-existing legal rules regulate all the facial/speech/text recognition technologies. This was also highlighted during discussions with LEA partners.

As each LEA is subject to different ethical, societal, and legal standards in their own countries, there is a need for them to be able to tailor compliance tools to their needs. This is particularly the case in terms of each legal jurisdiction regulating the activities of LEAs with separate legal regimes, and due to each organisation, and the populations policed by them, having different perspectives on ethical and societal issues.

Consequently, the decision-making mechanism presented below should be seen as a template designed with European-wide ethical, societal, and legal standards in mind, and can be adapted for use by LEAs to their particular context. The mechanism can, therefore, be seen as somewhat ‘neutral’ in the sense that it was designed at the Europe-wide level, and does not favour any particular ethical, societal, and legal regime within Europe.<sup>22</sup> ROXANNE partners recommend that if LEAs do modify the questions below, that they add additional considerations for the circumstances of their investigations, rather than remove questions, so that they can be

<sup>20</sup> Crootof, R. “The Killer Robots Are Here”, *Cardozo Law Review*, Vol.36, 2015, pp.1837-1915, pp.1864-1865.

<sup>21</sup> Scharre notes that the tasks which a machine is employed for are illustrative of how ‘autonomous’ it is. For example, a robotic assistant that walks with its owner can be seen to be more autonomous than having the same assistive functions in a robot that is designed to be stationary. See Scharre, P. *Army of None*, WW Norton & Company, New York, 2018, pp.27-32.

<sup>22</sup> Of course, this does not mean that the ROXANNE platform should be seen as a mere tool that is ‘neutral’ in terms of the impact of using it in the world. See Kranzberg, M., “Technology and History: “Kranzberg's Laws”” *Technology and Culture*, Vol.27, 1986, pp.544-560, p.545.

tailored to the specific needs of the individual LEAs. It is important that LEAs can adapt the decision-making mechanism to their needs, as the questions below should not be seen as a replacement for their current processes that ensure compliance with their current obligations.

Still, ROXANNE partners do acknowledge that the needs of some LEAs could result in more drastic modifications. When discussing the overall approach to this decision-making mechanism, a ROXANNE LEA partner noted that they would see greater utility in using the questions as training tools to make officer aware of key issues in their work which they would then be able to deal with as required, rather than within the framework of the mechanism.

Indeed, one of the criticisms of automated decision-making mentioned above is that it can be presented as ‘objective’ when, in reality, it is not. In the same way that algorithms cannot take into account all relevant data, the ROXANNE decision-making mechanism cannot cover all eventualities. In the same way that ROXANNE partners want to avoid having end-users follow the logic of the proposed ROXANNE platform, partners also want to avoid end-users following the logic of the decision-making mechanism without critical engagement, for example approaching it as a ‘tick-box’ exercise.

Therefore, each question has been provided with a rationale. This is to explain to end-users what the question is about, what issues it deals with, and why it is important. By conveying the importance of each question, and the underlying issues, this should enable investigators to better engage with the potential implications of their work, thereby raising the awareness of ethical, societal, and legal issues amongst LEA practitioners, but also avoiding risks of ‘functional autonomy’ and automation bias.

### 3. The decision-making mechanism

#### 3.1. Intended use

The intended use of the ROXANNE decision-making mechanism is for LEA officers to use it for assessing potential ethical, societal, and legal issues that could arise during the use of the proposed ROXANNE platform, or similar tools, and to demonstrate their compliance with the relevant standards. This serves several purposes. As mentioned above, it avoids situations of automated decision-making. It also facilitates greater awareness and engagement with the issues by investigators and avoids risks of functional autonomy and automation bias. Further, it enables uses and decisions to be logged for accountability purposes. Logging features are key to uncovering misuses of tools such as ROXANNE: if an LEA officer were to use the proposed platform for unethical or unlawful purposes, this would be logged and any investigation about such use will easily be able to see how the platform was used and make decisions accordingly.

Having end-users critically engage with relevant issues, and recording their answers to the questions within the decision-making mechanism adds benefits over simply logging uses and users. For example, an oversight body can assess the answers provided. This could be for a variety of purposes. A professional standards unit could assess whether LEA officers are adequately engaging with issues, both to find unprofessional activities (such as entering random text into answer boxes to simply complete the form), or to find examples of best practice (such as officers finding new issues that need to be considered). Further, any oversight body that needs to investigate criminal allegations of misconduct by an investigator, for example, should be able to gain insight into the mindset of an officer when using ROXANNE if they need to assess the intent of that investigator.

#### 3.2. Structure

During the development of the questions for the decision-making mechanism, it became clear that some questions needed to be asked before the ROXANNE platform was used, for example to assess privacy risks. Yet, other questions needed to be asked once results had been generated, to determine if a user properly understands the results, for example.

Following question development, they were grouped into questions best suited to be asked: at the procurement stage; when beginning a new case; when analysing new data, and; following data analysis. This approach was discussed with LEAs and technical partners who agreed that it was appropriate for dealing with the relevant issues, and could fit into current LEA structures. However, as noted above, actual implementation of the

decision-making mechanism would depend on the needs of the individual LEA and the ethical, societal, and legal standards that are best suited to their circumstances.

Where questions are presented below, they include reference to an ‘origin’. This is where the need for the relevant questions comes from. Many come from, and refer to specific section in, the previous ethical, societal, and legal analysis in D3.1 (Initial report on compliance with ethical principles), they are provided here to demonstrate a clear link with previous work and to evidence the necessity of including these questions. In the electronic version of the decision-making mechanism that will be included in the ROXANNE platform, these origins will not be included as it is not necessary for investigators to know where the questions originate from in the previous analysis and the salient information is included in that ‘rationale’ for each question. Still, end-users will still be able to access the present and previous documents should they wish to.

### 3.3. Decision-making at the procurement stage

From the beginning of LEAs using advanced technologies like ROXANNE, they should ensure that their policies and procedures for using them comply with the values held by the society that they police, and the ethical and legal standards that are applicable to them. Therefore, LEAs should consider the implications of using technologies such as ROXANNE when they procure them. The following questions should be included in any assessment carried out during the procurement process.

Ideally, LEAs procuring the proposed ROXANNE platform would be able to seek advice from an ethics board,<sup>23</sup> or experts in the ethical use of technologies in law enforcement. However, some LEAs might not have an ethics board, or might not wish to discuss technologies intended for sensitive policing operations outside of their organisation, and so decisions could be made by senior officers. In any case, the following questions should be considered as part of an assessment of technologies such as ROXANNE. This should be in addition to specific considerations of the relevant ethical, societal, and legal standards applicable to their circumstances. As these are questions that should be considered about the use of the ROXANNE platform overall, and not about specific uses of it, there is no need to include these questions in the electronic version of the decision-making mechanism.

Question	Rationale	Origin
Have you conducted a detailed assessment of the ethical, societal, fundamental rights, and legal impacts that could arise if your organisation used the ROXANNE platform?	It is important that LEAs have a comprehensive understanding of the issues that could be generated by their use of new technologies, and take steps to deal with any negative impacts	D3.1 generally.
What type of investigations would it be appropriate to use ROXANNE platform for? How will you prevent ‘function creep’?	The ROXANNE platform can cause intrusive effects on people’s privacy, and this should be limited to cases where such intrusions are necessary.  Further, the ROXANNE platform can process a lot of complex data, and use a lot of energy. Investigators should consider if another, less energy-intensive, tool can complete their task.	Ethics, use phase: privacy and data governance, ‘use of data’; Individual, societal, and environmental wellbeing.
How will you track the use of the ROXANNE platform? For example, should every LEA officer have a separate user account? Will you keep access logs?	Incorporating a logging system within the LEA organisation would allow senior LEA officers to monitor the use of the platform. Also, if each law enforcement representative has an individual account, they become	Ethics, Use phase, ‘Accountability’.

<sup>23</sup> See, for example, West Midlands Police and Crime Commissioner, “Ethics Committee”. Available at: <https://www.westmidlands-pcc.gov.uk/ethics-committee/>.



	accountable for their own actions.	
What oversight mechanisms/bodies will you implement with the users of ROXANNE?	<p>Oversight for technology use is crucial to ensure that ethical, societal, and legal standards are adequately applied before any potential violation, and to prevent poor standards resulting in unjustified violations.</p> <p>Oversight should exist within investigations from senior officers to ensure proper use of data analysis technologies, and from outside investigation teams to provide oversight of how standards are being applied.</p>	Ethics, Use phase, privacy and data governance, ‘use of data’.
What data security measures will be implemented with the ROXANNE platform? Will they adequately protect the data being analysed by ROXANNE, and the results?	<p>Data from LEA investigations is, by its nature, sensitive. It is imperative that it is kept secure in order to protect privacy, and the right to privacy.</p> <p>The Law Enforcement Directive (2016/680) requires that LEAs implement security appropriate measures to protect personal data against unauthorised/unlawful processing and accidental loss, destruction, or damage.</p> <p>It is important that data security measures are evidenced as significant harm could arise from a data breach.</p>	Ethics, use phase, Technical robustness and safety; Societal values, ‘Citizen privacy’; I v Finland App no 20511/03 (ECtHR, 17 July 2008), para.38-40; Art.4(1)(f), LED.
What will you do with personal data that is no longer needed? Will you provide a data retention policy to the public?	Personal data should be kept no longer than necessary (data minimisation principle); they should be anonymised or destroyed once they are no longer needed. In order to be transparent, the public should be informed about the data retention policy of LEAs.	Societal values, ‘Trust and the perception of safety’.
How confident are you about the results generated from this platform? Is the error rate acceptable for investigations?	LEAs should be confident in the efficacy of the technologies they deploy. This should include testing a system before deployment, and a determination if it is an appropriate tool for the operational environment. Where it is found to be inappropriate, for technical reasons or otherwise, it should not be deployed.	Societal values, ‘Unintended consequences of technological solutions’.
Do you have any reason to believe that the ROXANNE platform will produce biased effects on particular groups of people in your policing area? For example, are there populations whose data are disproportionately captured in investigations who could be discriminated against?	<p>The bias in algorithmic analysis can result in biased effects if they are acted upon and so data analysis tools should be evaluated for bias by users before they are deployed.</p> <p>Police data collection practices in the past have sometimes created biases, and the potential for them to affect ongoing</p>	Societal values, ‘Equality’.

	investigations needs to be considered.	
Do you think that the training modules provided for using with the ROXANNE platform are sufficient to make investigators aware about possible technical limitations? What training provision will you provide to demonstrate to users of ROXANNE that they should not simply ‘follow the algorithm’ but should critically evaluate their uses of the platform through the decision-making mechanism provided? How will you ensure that ROXANNE end-users are sufficiently trained so that they can comprehend the results of the ROXANNE analysis in order to explain them? Are there other trainings you think investigators should engage with before using ROXANNE?	<p>LEAs must be well informed about the possible technical limitations of the platform and what could possibly lead to an error prone conclusion from the system. Linked with the next question, it is also crucial that end-users are adequately trained in order that they can comprehend the results of the ROXANNE analysis.</p> <p>The ROXANNE platform is limited in its ability to analyse reality by the data that is uploaded to it. Investigators should not assume that the results of the ROXANNE platform accurately represent reality, nor that they are definitively correct; they are only an estimation that should be critically engaged with.</p>	Societal values, ‘Unintended consequences of technological solutions’; Societal values, ‘Respect for human life’.
How will you facilitate investigators explaining ROXANNE results, and how investigators reach conclusions, in court?	Judges and juries in criminal trials must have an accurate understanding of the evidence in order to weight it properly. Therefore, investigators should be able to adequately explain the results of the ROXANNE platform to judges and juries to ensure a fair trial.	Societal values, ‘Rule of law’; Ethics, use phase, Transparency.
Will you inform stakeholders (e.g. local citizens) about your intended uses of ROXANNE? Will your organisation gather views of stakeholders on how you intend to use the ROXANNE platform? Will you adapt your intended uses to comply with their views?	<p>In order to be transparent and avoid misunderstandings with the local population and build trust, LEAs should keep their stakeholders informed about the technologies they use in investigations.</p> <p>It is important that the use of ROXANNE-like technologies is evaluated by different groups, to ensure that they are used in ways that are acceptable to the communities that are being policed.</p>	Ethics, use phase, Individual, societal, and environmental well being; Societal values, ‘Trust and the perception of safety’
Do you intend to make your organisational privacy policies relevant to the use of ROXANNE public? Or have you done so?	LEAs should be transparent with the public about how they process data (whilst recognising operational needs), in order to build trust and allow to public to feel that their data is treated properly.	Societal values, ‘Social acceptability’; Societal values, ‘Unintended consequences of technological solutions’; Ethics, Transparency.
How can you avoid causing unnecessary harm to people whose data is analysed using ROXANNE?	People can feel distressed where they feel that sensitive data about them, or their acquaintances, has been processed without their knowledge. Unnecessary, and particularly intentional, harm	Fundamental rights, Art.4 Prohibition on torture.

	should be avoided, especially if it is used as a form of punishment or harassment outside of a formal legal process.	
How can you ensure that data-subjects will be supported if they experience distress after finding out about their data being processed by ROXANNE? Are there structures in place to support people who find out that they been subject to analysis by the ROXANNE platform?	LEAs should take care to ensure that they do not cause undue harm to person whose data are examined in investigations. People might find it distressing to learn that they have had their data analysed by the ROXANNE platform, for example if evidence is presented in court, it is important that the wellbeing of these people is supported.	Fundamental rights, Art.3 Integrity of the person; Ethics, use phase, Individual, societal, and environmental wellbeing.

### 3.4. Decision-making at the beginning of a new case

When investigators begin a new case using technologies such as ROXANNE, it is important that they assess issues relevant to its use across the investigation. The questions asked at this stage relate to issues that can affect an entire investigation. Therefore, they only need to be asked once at the beginning of a new case. Specific issues related to the data to be analysed are asked in the next stage. As these questions relate to an entire investigation, it recommended that they be considered by a senior officer within the investigation.

Question	Rationale	Origin
Please confirm that you understand that the ROXANNE platform is intended to provide assistance to LEA officers, and decision-making should not be delegated to it.	The ROXANNE platform is not capable of making decisions in investigations. LEA officers should not just follow the results outputted, but should use them as information to make decisions-from. Investigators should take account of the context when understanding the results of the analysis; for example, highlighting a person has being in a communication network with known criminals does not indicate that they are involved in illegal activity.	Ethics, Use phase, Human dignity, ‘Alienation’.
Please confirm that you are aware that the results of the ROXANNE platform are an estimation, and are not conclusive. Results should be assessed once analysis is completed.	The ROXANNE platform can recognise patterns in investigation data. Therefore, it can highlight data points to pay attention to, but cannot provide information on why. Further, the ROXANNE platform was developed in a research project and so the algorithms ‘out of the box’ are not specifically trained on LEA investigation data.	Ethics, use phase, Technical robustness and safety.
Please confirm that you are using ROXANNE in accordance with your organisational policy on data security.	Given the sensitive nature of the data, and the suggestion that data security is considered at the procurement stage, investigators should attest that they are using the correct data security procedures to avoid any data leaks or unauthorised access.	Ethics, use phase, Technical robustness and safety; Ethics, use phase, Technical robustness and safety; Societal values, ‘Citizen privacy’; I v Finland App no 20511/03 (ECtHR, 17 July 2008), para.38-40.
Are you processing the data for	It is important that LEAs process	Arts.1(1), 4(1)(b), 4(2),

<p>law enforcement purposes? What is your specific purpose?</p>	<p>investigative data under an appropriate legal basis. The Law Enforcement Directive (2016/680) states that law enforcement purposes are the <i>‘prevention, investigation detection or prosecution of criminal offences or the execution of criminal penalties,[...] and the prevention of threats to public Security.’</i></p> <p>The LED also requires that these purposes are <i>‘explicit, specified, and legitimate’</i>.</p> <p>If data are process for non-law enforcement purposes, then this should be regulated under the GDPR (unless allowed in member state law).</p>	<p>4(3), 8, and 9, LED.</p>
<p>What is your lawful basis for analysing the data? Provide European Union and Member State law as required, and highlight if these are separate legal bases for processing data of different categories of people.</p>	<p>A violation of privacy should only take place where it is proportionate, lawful, and subject to effective oversight. Ensuring that data is processed according to the law is important as it prevents investigators going beyond their powers. The Law Enforcement Directive requires that purposes of data processing are lawful and fair.</p> <p>Under human rights law, the European Court requires that domestic law provides measures to protect persons who are incidentally recorded in surveillance data. To ensure that any infringement of the right to privacy is lawful, there must be a basis in domestic law and this should be recorded .</p>	<p>Ethics, Use phase, privacy and data governance, ‘use of data’; Arts. 1(1), 4(1)(a) and 10, LED; Fundamental rights, Art.7, Respect for private and family life; Amann v Switzerland App No 27798/95 (ECtHR, 16 February 2000), Para.61; Fundamental rights, Art.8 protection of personal data.</p>
<p>Is it necessary to use the ROXANNE platform for this investigation ?</p>	<p>The ROXANNE platform can process a lot of complex data, and use a lot of energy. This raises risks of violating privacy and spending a lot of energy.</p> <p>Investigators should consider if another, less intrusive or less energy-intensive, tool/process can complete their task.</p>	<p>Ethics, use phase: privacy and data governance, ‘use of data’; Individual, societal, and environmental wellbeing.</p>
<p>Which person/body oversees this data analysis in this specific operation?</p>	<p>A violation of privacy should only take place where it is proportionate, lawful, and subject to effective oversight. Oversight for technology use is crucial to ensure that privacy issues are adequately considered before any potential violation, and to prevent poor standards resulting in unjustified violations.</p>	<p>Ethics, Use phase, privacy and data governance, ‘use of data’.</p>
<p>Have the persons who will be using the ROXANNE platform in the investigation completed</p>	<p>Training should cover several areas including transparency (understanding how the system produces results), human</p>	<p>Ethics, Use phase, privacy and data governance, ‘use of data’.</p>



<p>the required training provision?</p>	<p>rights protections and accountability procedures.</p> <p>Investigators should be adequately trained in both using ROXANNE, and the potential impacts it can produce.</p>	
<p>Will you limit access to investigative data to certain investigators within the investigation? How will you limit access (e.g. need-to basis, rank)?</p>	<p>Personal data in investigations should only be accessed by people who need to do so for legitimate purposes. Where highly sensitive data is processed, investigations should consider if this needs to be sequestered in some way.</p>	<p>Societal values, ‘Citizen privacy’.</p>
<p>Regarding transferring data between investigations, do you envisage:</p> <p>a) Transferring data from your investigation to another investigation?</p> <p>b) Transferring data from another investigation into yours?</p> <p>Why? Is this necessary? Is this lawful? Who will oversee, and provide authorisation for, this?</p>	<p>Provision of sensitive data to other persons, or organisations, who do not need access is an additional violation of privacy, it therefore needs to be proportionate, lawful, and subject to oversight.</p>	<p>Ethics, use phase, privacy and data governance, ‘use of data’.</p>
<p>Is the data processing expected in your investigation in compliance with your organisational data protection policy (ideally made public)?</p>	<p>In order to remain transparent, the public should be able to generally determine how their data will be used by LEAs.</p>	<p>Societal values, ‘Social acceptability’; Societal values, ‘Unintended consequences of technological solutions’; Ethics principles, Transparency.</p>
<p>How will you integrate use of the ROXANNE platform into your investigation alongside ‘ordinary’ (i.e. non-data-driven) decision-making approaches? How will you verify the results of the ROXANNE platform?</p>	<p>End-users should be aware that data-analysis platforms may give results that could be biased, erroneous, and difficult to understand, depending upon the data inputted. LEA officers leading investigations should be clear on how they will deal with these issues, if they arise. Senior officers should ensure that user maintain a critical interpretation of results from data analysis platforms.</p>	<p>Fundamental rights, Art. 21 Non-discrimination.</p>
<p>Do you foresee a risk of biased data, or biased effects? What steps could you take to mitigate these risks?</p>	<p>Having biased data sets is a risk investigators face when they analyse investigative data with technologies.</p> <p>It is important that senior officers are aware of these risks and how it could affect investigations. It is also important that they take steps to mitigate bias risks not only to avoid discriminatory policing, but also to avoid leading their investigation down an erroneous path.</p>	<p>Fundamental rights, Art. 21 Non-discrimination.</p>
<p>Are you in a position to fulfil the rights of data-subjects, if</p>	<p>The Law Enforcement Directive has fewer data-subject rights than the</p>	<p>Ethics, Use phase, privacy and data governance, ‘use</p>

needed?	GDPR, <sup>24</sup> and the exercise of these rights is restricted under certain conditions. <sup>25</sup> Investigators should be cognisant that data-subjects might be able to access data held about them in future and could use their data as a tool to hold investigators accountable for errors.	of data’.
If people discovered how you intend to process their personal data, would they likely act differently? For example, would they express themselves, or interact with others, differently? How big of an impact could this create? Would this be a necessary and proportionate interference with freedom of expression, and freedom of assembly and association?	<p>LEA activity can result in innocent people acting different due to ‘chilling effects’. In terms of freedom of expression, people might self-censor themselves to avoid attracting LEA attention. Self-censorship due to a fear of unnecessary court proceedings initiated by authorities can violate the freedom of expression.</p> <p>In terms of the freedom of assembly and association, people might not associate with certain people either to avoid implicating themselves or their associates in the eyes of LEAs. Unlawful, temporary, and mistaken LEA interest have all resulted in violations of freedoms of association where they affected how people associate with each other.</p> <p>Investigators should ensure that any potential impact on the behaviour of people is necessary and proportionate.</p>	<p>Maegulev v Russia, App No 15449/09 (ECtHR, 8 January 2020); Christian Democratic People’s Party v. Moldova App No 28793/02 (ECtHR, 14 May 2006), para.77; Nurettin Aldemir and Others v. Turkey App Nos 32124/02, 32126/02, 32129/02, 32132/02, 32133/02, 32137/02 and 32138/02 (ECtHR, 2 June 2008), para.34; The United Macedonian Organisation Ilinden and Ivanov v. Bulgaria App No 44079/98 (ECtHR, 15 February 2006), para.135; Bączkowski and Others v. Poland App No 1543/06 (ECtHR, 24 September 2007), paras.66-68.</p>
How will you manage data once your investigation is completed? Will you anonymise, or destroy, the data? If you do not know, when will you review this decision?	The Law Enforcement Directive requires that data-subjects should only be identifiable for as long as is necessary for law enforcement purposes. When they are no longer needed, they should be anonymised or destroyed	Art.4(1)(e), LED.
Do you intend to publish a purple notice based on information detected using the ROXANNE platform?	Purple notices are published to warn about modi operandi used by offenders or request information on offences to resolve or assist LEAs in their investigation. With ROXANNE this kind of intelligence may be collected when using the platform and shared further on with the use of purple notices.	Art. 92, INTERPOL Rules on the Processing of Data (RPD, further information on this topic will also be included in D3.3 (INTERPOL Global Communications Infrastructure)).
Are the facts subject to the purple notice still under investigation or not?	Depending on the status of the facts (under investigation or no longer under investigation), the INTERPOL Rules on the Processing of Data define different conditions for the publication of the purple notice.	Art. 92, RPD

<sup>24</sup> Chapter III, LED

<sup>25</sup> Art.15, LED

### 3.5. Decision-making when using new data

When LEAs bring new data into an investigation, it is important that they assess the risks and implications of analysing the data prior to processing it. As mentioned above, the analysing of data in an investigation can be considered an additional infringement on privacy beyond an infringement at the point where the data is collected. Therefore, investigators should consider the issues related to their specific use of the data, and whether they need to process it. The questions at this stage could be answered by investigators (potentially junior officers) who actually use the ROXANNE platform, in distinction to the suggestion that officers leading an investigation should complete the previous set of questions.

The need to separate out questions between those that should be asked at the beginning of a case, and those when new data is brought into an investigation was discussed with ROXANNE LEA partners who agreed that there were distinct issues at each stage that need to be considered separately. Consequently, the questions in this section should be considered every time new data is brought into an investigation.

Question	Rationale	Origin
Are you an investigator assigned to the case which these data relate? What is your purpose in processing these data?  If you are not assigned to the case which these data relate to, what purpose are you accessing these data for?	It would seem to be an unjustified violation of privacy if people from outside an investigation can access sensitive data without good reason.	Ethics, Use phase, privacy and data governance, ‘use of data’.
What are your details? Name, rank, ID number, etc. <sup>26</sup>	It is important that any person who decides on a violation of privacy is accountable for their actions, and can be questioned about their reasoning for this.	Ethics, Use phase, privacy and data governance, ‘use of data’
Was a warrant required to collect these data? What is the warrant number? Are there any restrictions regarding data-analysis from this warrant? Are there any details you should note here?	A violation of privacy should only take place where it is proportionate, lawful, and subject to effective oversight. Ensuring that data is processed according to the law is important as it prevents investigators going beyond their powers.  The collection and processing of sensitive data is often authorised by a judge providing a warrant, especially when gathered by covert means. This is an opportunity to attest that a judge has authorised certain actions.	Fundamental rights, Art.8 Protection of personal data.
What is the nature of the data you intend to process?	Investigators should clearly document the types of data they want to process	Z v Finland App No 22009/03 (ECtHR, 25 February 1997).
Are the data factual, or are they based on personal assessments (e.g. witness statements)? If there is a mix, please provide details.	The Law Enforcement Directive requires that LEAs distinguish, as far as possible, personal data based on fact and that based on personal assessments, such as witness statements. This question gives an	Art.7, LED.

<sup>26</sup> Depending upon if users of the ROXANNE platform are logged automatically, information on platform users could also be recorded automatically. In which case, this question would not be needed.

	opportunity to do this.	
What categories of data-subject are included in the dataset? (e.g. suspects, convicts, victims, witnesses.)	The Law Enforcement Directive requires that LEAs should make a distinction between categories of data-subjects. This question provides an opportunity to do this.	Art.6, LED.
Does the dataset contain special category data?	<p>Special category data is that which reveals ‘<i>racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation</i>’.</p> <p>Such data can only be processed where it is allowed by law, to protect someone’s vital interest, or where it has been made manifestly public by the data-subject.</p>	Art.10, LED.
Is the data adequate, relevant and limited to your purposes? Do you need to analyse the data of all persons represented in the dataset? Could you partition the data in some way? What are you planning to do with the irrelevant data?	<p>Ethical considerations require that investigators consider if people who are unconnected to an investigation, but are captured in a dataset, could be removed from the analysis to avoid potential violations of privacy.</p> <p>With regard to data protection law, the Law Enforcement Directive requires that personal data to be processed is only that which is adequate, relevant, and not excessive for the processing (data minimisation principle). So, for example, data about people not connected to an investigation should not be processed as part of an investigation; LEAs should anonymise or destroy data that is not needed.</p> <p>In terms of human rights law, the privacy rights of both the sender and receiver of communications can be infringed when analysing communication data. Investigators should ensure that they do not unnecessarily analyse personal data.</p>	Ethics, use phase, Individual, societal, and environmental wellbeing; Art.4(1)(c), LED; Fundamental rights, Art.7, Respect for private and family life; Lamber v France App No 23618/94 (ECtHR, 24 August 1998), Para.21; Iordachi and Others v Moldova App No 25198/02 (ECtHR, 14 September 2009), para.44.
Is the data accurate? Is it up-to-date?	The Law Enforcement Directive requires that data is accurate and up-to-date, and that inaccurate data should be erased or rectified without delay.	Art.4(1)(d), LED.
Is the data of adequate quality to be analysed? How will you evaluate results to account for any errors caused by poor-	Poor quality data can be present in investigations where, for example, data comes from old surveillance cameras, or misplaced covert microphones.	Ethics, Use phase, privacy and data governance, ‘use of data’.

quality data?	Poor quality data might result in erroneous results, and these should be screened out by investigators.	
Does this dataset include data about children? What additional measures will you take when processing their data (e.g. additional security measures, processing only by authorised staff)?	LEA data processing of personal data is regulated under the Law Enforcement Directive, but its sister regulation, the GDPR, explicitly states that children's personal data merits additional protection. This is in conformity with human rights law which provides special protection to children.	Fundamental rights, Art.24 The rights of the child; Information Commissioners Office's guide on Children and the GDPR
Are there any risks of bias in the processing of this dataset?	If a particular dataset has a bias towards a particular demographic of the society, the same might be reflected in the conclusions of the platform. There should be a conscious effort to appreciate risks of bias in data processing and avoid creating biased effects in the real world.	Societal values, 'Unintended consequences of technological solutions'.
Are you likely to be processing data about people's private or family lives? How will you safeguard people's privacy during your processing?	The right to privacy is an important right in intrusive investigations, so investigators must be clear on how they will protect this right.	Fundamental rights, Art.7 Respect for private and family life.
Would the people whose data you intend to process expect it to be private?	LEAs should consider whether people whose data they are processing would expect their data to be processed in the way you intend.	Krone Verlag GmbH v Austria App no 431/96 (ECtHR, 26 February 2002); Von Hannover v Germany App no 59320/00 (ECtHR, 24 June 2004).
Why is it necessary to process data about people's private lives in this case and in this way?	For an infringement on the right to privacy to be lawful, it must be necessary. Processing that violates privacy is likely to damage trust in LEAs.	Fundamental rights, Art.7 Respect for private and family life (Art.8(2), European Convention on Human Rights); Societal values, 'Trust and the perception of safety'.
What is your aim in processing this data, what are you trying to achieve? Is this a legitimate aim? If you are violating someone's privacy, is it proportionate to the crime(s) under investigation? Could you reach the same goal in a less intrusive way?	For an infringement on the right to privacy to be lawful, it must be proportionate to a legitimate aim.  In ethical terms, a violation of privacy should only take place where it is proportionate, lawful, and subject to effective oversight. It is important to demonstrate that any violation of privacy is proportionate to the ongoing investigation and that there is no less intrusive way of completing the task.	Ethics, Use phase, privacy and data governance, 'use of data'; Fundamental rights, Art.7 Respect for private and family life.
Which tools in the ROXANNE platform do you need to use? Do you need to use all of them?	Use of each ROXANNE tool could result in infringement of privacy, and so investigators should only use the tools that they need to.	Fundamental rights, Art.7, Respect for private and family life.
Can the person whose data you	Investigators should endeavour to allow	Leander v Sweden App no



are processing access the data you have about them?	data-subjects to access their data when legally permitted whilst not causing damage to investigations.	9248/81 (ECtHR, 26 March 1987); Gaskin v UK App no 10454/83 (ECtHR, 7 July 1989), para.49.
How is your data processing using this tool subject to oversight?	Oversight of activities that engage human rights is important to ensure that standards that allow for infringement are properly considered.	Klass v Germany App no 5029/71 (ECtHR, 6 September 1978).

### 3.6. Decision-making after data has been analysed

Once investigators have completed their analysis and are considering the results, it is important that they take steps to understand them thoroughly, and consider them in the relevant context. The below questions should be asked after each session using ROXANNE platform to ensure that the results of the data analysis are properly evaluated, and issues regarding potentially innocent people whose data are included in the investigation are considered. Each session could include analysing a lone dataset, or several data types (whether sequentially or simultaneously). It would seem overly-onerous to expect investigators to consider these questions after analysing each dataset if there are several datasets being analysed together, especially where conclusions related to the case might only be drawn after viewing the results of analysing several datasets together. Therefore, it was decided to ask these questions at the conclusion of each user session when using the proposed ROXANNE platform.

Question	Rationale	Origin
How confident are you that the results are accurate? Reliable? Precise?	It is important that results of the ROXANNE platform are critically evaluated. Acting on erroneous results could result in innocent people being investigated, or offenders remaining free.	Ethics, use phase, Technical robustness and safety.
Can you understand the results of the ROXANNE platform?	Investigators must understand the results of the ROXANNE platform before acting on them so that risks of investigation or arrest of innocent people are not realised, and that actual perpetrators can be apprehended quicker.	Societal values, Rule of law.
Can you foresee any issues that could arise for understanding these results, for example if they are presented in court?	If it is not possible to understand the results of the platform, this could affect the ability of the defence to challenge evidence if it is presented in court.	Fundamental rights, Art.47 Right to an effective remedy and a fair trial; Societal values, 'Transparency'.
Will you remove people from the dataset who are shown to be innocent in these results? If yes how? If no, why not?	Innocent people should be protected from intrusive investigations, particularly where they are unnecessary.	Fundamental rights, Art.48 Presumption of innocence and right of defence.
How will you assess the outputs of the platform before acting on them?	The user should be aware that as the platform cannot comprehend context and so cannot differentiate between, for example, innocent communications between family and the communications of a criminal organisation. Therefore the user should critically assess the results of the ROXANNE platform to ensure they are properly understood before they are	Fundamental Rights, Art. 22 Cultural, religious and linguistic diversity.

	acted upon.	
How will you validate, or corroborate, the results of the ROXANNE platform? For example, replaying audio to check voice identification, reading transcripts to validate text analysis results, or checking connections made in network analysis?	LEAs highlighted that they would like to be able to validate the results of the ROXANNE platform. Investigators should be provided with opportunity to attest to doing this so as to show that they have engaged with investigation data and are not ‘following the algorithm’.	ROXANNE requirement answers. end-user survey
Is there anything unusual/unexpected in these results?	It is important to identify obvious errors in order that they can be considered to determine if there are actually errors, or just unexpected results.	Ethics, use phase, Technical robustness and safety.
Have you considered how this analysis could be wrong?	The ROXANNE platform is limited in its ability to analyse reality by the data that is uploaded to it. Investigators should not assume that the results of the ROXANNE platform accurately represent reality, nor that they are definitively correct; they are only an estimation.	Societal values, ‘Respect for human life’.

## 4. The decision-making mechanism in electronic form

An initial mock-up of the decision-making mechanism in electronic form has been created, and a complete version should be integrated with the rest of the ROXANNE platform for the upcoming mid-point review of the project in May 2021, where it will be demonstrated alongside other parts of the platform.

### 4.1. Technical and design specification

The decision-making mechanism will sit within the ROXANNE platform as a component to work alongside those from technical partners. Where an end-user begins a new case, adds new data, or completes a session, the relevant series of questions should be automatically presented to the user to complete (as discussed above, those questions related to LEA activities at the procurement stage do not need to be included in the platform itself and so will not be recreated in electronic form). The decision-making mechanism will screen answers to ensure that end-users enter words that are found in the dictionary; e.g., a user who enters ‘qwerty’ or ‘123456’ will be prompted to provide substantive answers to the questions posed.

Once answers are provided, they will be saved in a file and associated to the case and dataset that they relate to. Depending on how the completed component works, the answers will either be saved in a separate file or as meta-data. This information will be available to oversight bodies for any investigations/checks. Further, partners are considering having the ability to associate the answers of a user to previous cases in case an oversight body wishes to look into the previous actions of a specific user of the ROXANNE platform.

Visually, the completed decision-making mechanism will match the aesthetic of the ROXANNE project, such as that on the project website.<sup>27</sup> Additionally, the design of the decision-making mechanism will follow the dissemination requirements in Article 29 of the ROXANNE Grant Agreement to include an EU emblem logo, and the following text ‘This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 833635’.

<sup>27</sup> ROXANNE project, “Home”, 2020. Available at: <https://roxanne-euproject.org/>

## 4.2. Mock-up of the decision-making mechanism

This electronic form will thus present the questions of the decision-making mechanisms detailed above in order to collect the responses of end users when beginning a new case, introducing new data, or following their analysis. Before providing the final version of this electronic form, mock-up work has been started. Below, the human-machine interfaces presenting the different questions of the decision mechanism are presented.



Co-funded by  
the European Union



---

### Pre-analysis (new case):

The question of this stage cover issue that will affect an entire investigation, and so should only need to be asked once .

**\* Required**

Please confirm that you understand that the ROXANNE platform is intended to provide assistance to LEA officers, and should not be used to make decision for you. \*

The ROXANNE platform is not capable of making decisions in investigations. LEA officers should not just follow the results outputted, but should use them as information to make decisions-from. Investigators should take account of the context when understanding the results of the analysis; for example, highlighting a person has being in a communication network with known criminals does not indicate that they are involved in illegal activity.

Yes

No

Please confirm that you are aware that the results of the ROXANNE platform are an estimation, and are not conclusive. \*

The ROXANNE platform can recognize patterns in investigation data. Therefore, it can highlight data points to pay attention to, but cannot provide information on why. Further, the ROXANNE platform was developed in a research project and so the algorithms 'out of the box' are not specifically trained on LEA investigation data.

Yes

No

Figure 1: Cover page and start of the 'new case' questionnaire



### Post-analysis:

These questions should be asked after each use of the ROXANNE platform to ensure that the results of the data analysis are properly evaluated, and issues regarding potentially innocent people whose data are included in the investigation are considered.

#### How confident are you that the results are accurate? Reliable? Precise? \*

It is important that results of the ROXANNE platform are critically evaluated. Acting on erroneous results could result in innocent people being investigated, or offenders remaining free.

Your answer

---

#### Can you understand the results of the ROXANNE platform? \*

Investigators must understand the results of the ROXANNE platform before acting on them so that risks of investigation or arrest of innocent people are not realized, and that actual perpetrators can be apprehended quicker

Yes

No

#### Can you foresee any issues that could arise for understanding these results, for example if they are presented in court? \*

If it is not possible to understand the result of the platform, this could affect the ability of the defence to challenge evidence if it is presented in court.

Yes

No

Figure 2: Post-analysis questionnaire

Please confirm that you are aware that the results of the ROXANNE platform are an estimation, and are not conclusive. \*

The ROXANNE platform can recognize patterns in investigation data. Therefore, it can highlight data points to pay attention to, but cannot provide information on why. Further, the ROXANNE platform was developed in a research project and so the algorithms 'out of the box' are not specifically trained on LEA investigation data.

Yes


No

Please confirm that you are using ROXANNE in accordance with your organizational policy on data security. \*

Given the sensitive nature of the data, and the suggestion that data security is considered at the procurement stage, investigations should attest that they are using the correct data security procedures to avoid any data leaks or unauthorized access.

Yes

No

 This is a required question

Are you processing the data for law enforcement purposes? \*

It is important that LEAs process investigative data under an appropriate legal basis. The Law Enforcement Directive (2016/680; LED) states that law enforcement purposes are the 'prevention, investigation detection or prosecution of criminal offences or the execution of criminal penalties,[...] and the prevention of threats to public Security.' The LED also requires that these purposes are 'explicit, specified, and legitimate'. If data are process for non-law enforcement purposes, then this should be regulated under the GDPR (unless allowed in member state law).

Yes

No

Figure 3: Checking end-users results

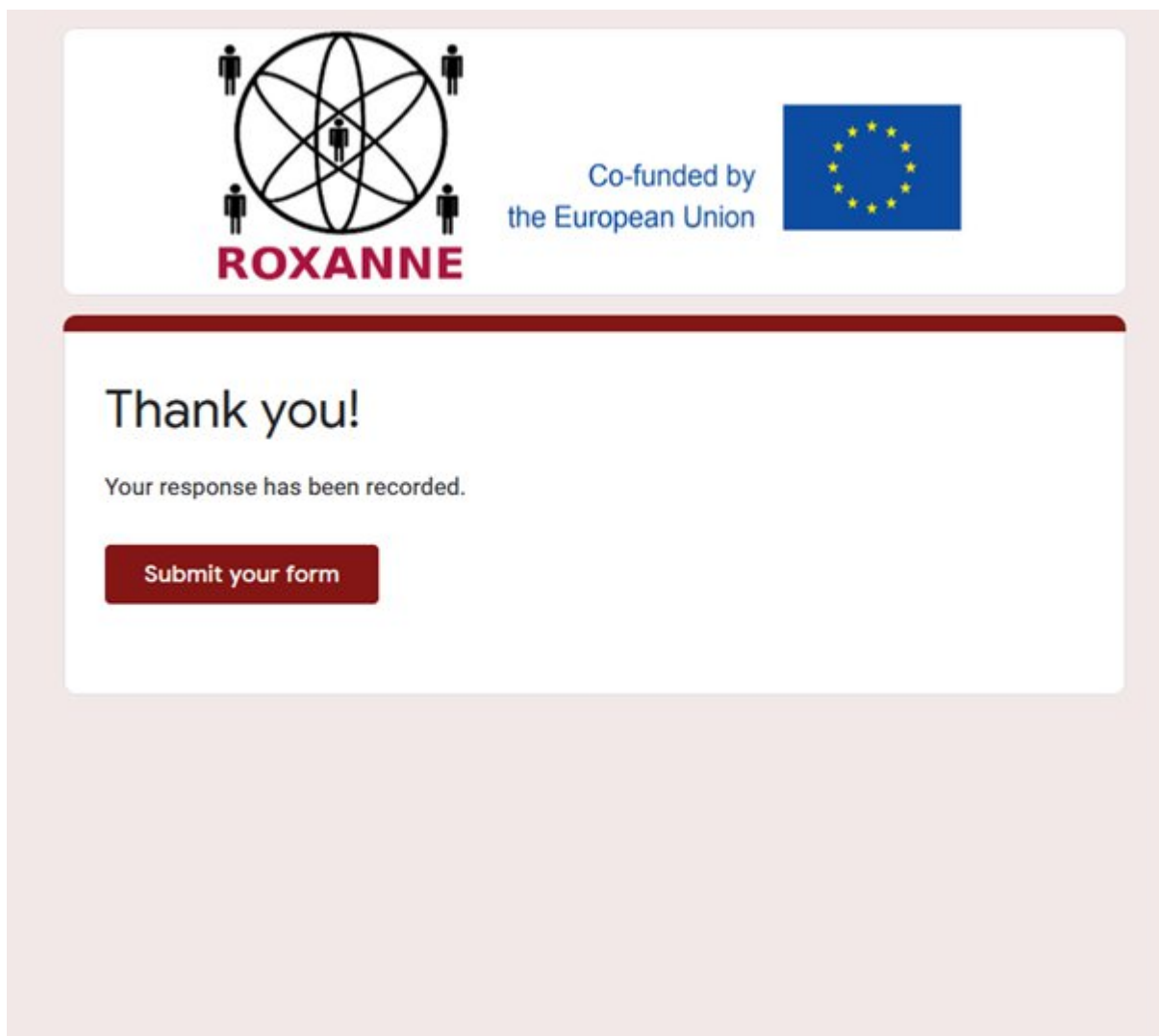


Figure 4: End of questionnaire and submission of results

## 5. Sending Decision-making mechanism to Data Protection authorities

The last part of this task is to send the decision-making mechanism to ‘Data Protection Officer organisations’ in project partner countries. The project partners interpret this to be Data Protection Authorities in partner countries. The partners will send an edited version of this deliverable to them, and request feedback. In order that the project disseminates this information as wide as possible, the partners will also send the same document to all other Data Protection Authorities in the EU and EEA even where they are not represented in the consortium, and the European Data Protection Supervisor, in order to elicit the greatest amount of feedback possible.

### 5.1. Authorities chosen

The following authorities have been selected to be provided with the decision making mechanism (most of these are members of European Data Protection Board<sup>28</sup>), and will be requested to provide feedback.

1. Austria: Österreichische Datenschutzbehörde

<sup>28</sup> European Data Protection Board, ‘Members’, 2020. Available at: [https://edpb.europa.eu/about-edpb/board/members\\_en](https://edpb.europa.eu/about-edpb/board/members_en)

2. Belgium: Autorité de la protection des données - Gegevensbeschermingsautoriteit (APD-GBA)
3. Bulgaria: Commission for Personal Data Protection
4. Croatia: Croatian Personal Data Protection Agency
5. Cyprus: Commissioner for Personal Data Protection
6. Czech Republic: Office for Personal Data Protection
7. Denmark: Datatilsynet
8. Estonia: Estonian Data Protection Inspectorate (Andmekaitse Inspektsioon)
9. Finland: Office of the Data Protection Ombudsman
10. France: Commission Nationale de l'Informatique et des Libertés - CNIL
11. Germany: Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
12. Greece: Hellenic Data Protection Authority
13. Hungary: Hungarian National Authority for Data Protection and Freedom of Information
14. Ireland: Data Protection Commission
15. Italy: Garante per la protezione dei dati personali
16. Latvia: Data State Inspectorate
17. Lithuania: State Data Protection Inspectorate
18. Luxembourg: Commission Nationale pour la Protection des Données
19. Malta: Office of the Information and Data Protection Commissioner
20. Netherlands: Autoriteit Persoonsgegevens
21. Poland: Urząd Ochrony Danych Osobowych (Personal Data Protection Office)
22. Portugal: Comissão Nacional de Proteção de Dados - CNPD
23. Romania: The National Supervisory Authority for Personal Data Processing
24. Slovakia: Office for Personal Data Protection of the Slovak Republic
25. Slovenia: Information Commissioner of the Republic of Slovenia
26. Spain: Agencia Española de Protección de Datos (AEPD)
27. Sweden: Datainspektionen
28. Iceland: Persónuvernd
29. Liechtenstein: Data Protection Authority, Principality of Liechtenstein
30. Norway: Datatilsynet
31. United Kingdom: The Information Commissioner's Office
32. Switzerland: Office of the Federal Data Protection and Information Commissioner (FDPIC)
33. Israel: The Privacy Protection Authority
34. European Data Protection Supervisor

## 5.2. Opportunity for feedback/validation

After sharing the documentation related to the decision making mechanism, we intend to collect feedback from all the above authorities over e-mail. Where relevant, this feedback will be reported as part of D3.4 and any changes to be incorporated into the decision making mechanism will also be noted there.

## 6. Conclusion

This deliverable explains the nature of human decision-making for using the proposed ROXANNE platform, and that all decisions should be made by human beings. Further, those decisions should not be subject to ‘functional autonomy’, or ‘automation bias’. In order to prevent these situations happening, end-users should critically engage with the ethical, societal, and legal issues that are relevant to their use of the ROXANNE platform. The questions offered above should facilitate that engagement and enable LEA officers to be fully cognisant of the issues related to their processing. Finally, it has been explained that the project partners will seek feedback on the above decision-making mechanism from European Data Protection Authorities.