Deliverable N° 9.2

Title: Incidental Findings Policy (WP9)

Start date of the project: **1/8/2018** / Duration: **36 months**

Planned delivery date: 31/10/2018

Submission date: 31/10/2018

Work package: WP9/Task:9.2

Work package leader: UAB

Deliverable leader: UAB

Version: Final

Dissemination level	(√ where appropriate)
Public	v
Classified, as referred to Commission Decision 2001/844/EC	
Confidential, only for members of the consortium (including the Commission Services)	

Version 19
Date: *29/10/2019*

Author(s):

P.Casanovas
Nicholas Morris
Emma Teodoro
Jorge González-Conejero
Rebeca Varela Figueroa
With the cooperation of Rick Adderley

European Commission | Horizon 2020 European Union funding for Research & Innovation

Project funded by H2020 Programme – Grant Agreement number: 786993

VERSION	MODIFICATION(S)	DATE	AUTHOR(S)
01	Conceptual scheme of identified risks (Data Protection Impact Analysis)	15/09/2018	Emma Teodoro (UAB)
02	State of the art (literature)	18/09/2018	Pompeu Casanovas (UAB-La Trobe)
03	Statistical matrix	20/09/2018	Nicholas Morris (UAB-La Trobe)
04	Risk analysis	20/09/2018	Nicholas Morris (UAB-La Trobe)
05	Police Findings (UAB Questionnaire)	08/10/2018	Emma Teodoro (UAB)
06	Incidental findings and residual risks in security environments	13/10/2018	Pompeu Casanovas (UAB-La Trobe)
07	Risk Matrix	14/10/2018	Nicholas Morris (UAB-La Trobe)
08	Risk identity analysis	14/10/2018	Pompeu Casanovas (UAB-La Trobe)
09	LEA's answer's analysis	15/10/2018	Pompeu Casanovas (UAB-La Trobe)
10	Questionnaire as annex	15/10/2018	Nicholas Morris (UAB-La Trobe)
11	Recommendations	16/10/2018	Pompeu Casanovas (UAB-La Trobe)
12	Ethical review (EAB comments)	18/10/2018	Ugo Pagallo (EAB Member)
13	Ethical review (EAB comments)	18/10/2018	Liliana Mitrou (EAB Member)
14	Adjustments to questionnaire in response to Ethical Committee comments	19/10/2018	Nicholas Morris (UAB-La Trobe)
15	Adjustments to Deliverable in response to EAB comments	21/10/2018	Pompeu Casanovas (UAB-La Trobe)
16	Ethical Comments EAB	28/10/2018	David Watts (EAB Member), Giovanni Sartor (EAB Member), Virginia Dignum (EAB Member)

European Commission | Horizon 2020 European Union funding for Research & Innovation

Project funded by H2020 Programme – Grant Agreement number: 786993

17	Adjustments to Deliverable in response to EAB comments	30/10/2018	Pompeu Casanovas (UAB-La Trobe)
18	Review	31/10/2018	Nicholas Morris (UAB-La Trobe), Pompeu Casanovas (UAB-La Trobe), Emma Teodoro (UAB-IDT) and Jorge Gonzalez-Conejero (UAB-IDT)
19	Update following comments from the mid-term review	29/10/2019	Rebeca Varela (UAB-IDT)
20	Final Review	21/02/2020	Nicholas Morris (UAB-La Trobe) and Pompeu Casanovas (UAB-La Trobe)

Table of Contents

European Commission | Horizon 2020 European Union funding for Research & Innovation

Project funded by H2020 Programme – Grant Agreement number: 786993

1. Executive Summary

Deliverable D9.2 follows the *Reply to the Ethics Second Assessment Report*, submitted on April 30th. (We will refer to this document when necessary). It contains a set of measures for the reduction of incidental findings and residual risks: (i) a policy for re-identified data, (ii) a privacy preserving algorithm development, (iii) a Privacy by Design (PbD) approach, (iv) an incidental risks mitigation policy. It also contains the results of a first consultation to LEAs.

Following the recommendations received at the mid-term review, this Deliverable has been updated. The update includes the results of the first consultation with LEAs (Section 5.4) and the report on the second consultation with LEAs (Sections 5.5 and 5.6.) and a clarification on the scope of the Deliverable.

As for the clarification, it is important to note here that:

1) The risks identified in this Deliverable are subject to an ongoing monitoring process specifically designed for Spirit that includes internal and external monitoring processes and bodies (DPO, EAB). The monitoring processes and bodies have been set up on the reports prepared for the ethical review and in Deliverables 9.1 to 9.5 and future iterations. The results of this monitoring, until M12, are reported in Deliverable 9.5.

2) However, this monitoring is also part of the general risk management strategy that contains a list of hazards, the risk assessment, and monitoring and mitigation measures identified, in D1.5 (M16) and its later iterations.

Against this background, D9.2 describes the operation of a spreadsheet-based model which seeks to calculate the overall risks which may be faced by the SPIRIT system, both before and after policies have been implemented to mitigate these risks. The model has yet to be calibrated using data on each of the risks – a process which will require considerable resources and time – but in order to illustrate the working of the model, we have populated it with example, very preliminary, guesstimates.

Incidental risks are the risks of misuse of the system caused by internal and external factors. These risks can be mitigated (reduced) by the use of suitable *policies*. The risks that remain after these policies have been implemented and taken full effect are termed *residual risks*.

In order to identify possible sources of incidental risks we have reviewed privacy and data protection inquiries, press coverage, and the academic literature on the subject. This investigation has focused particularly on the recent literature and experience following the introduction of new European

Project funded by H2020 Programme – Grant Agreement number: 786993

data protection regulations, the General Data Protection Regulation (GDPR) in 2016 (enacted on May 25th 2018), and the Directive (EU) 2016/680 on the prevention, investigation, detection or prosecution of criminal offences.

We have grouped the incidental risks into five *sources* – those emanating from Individual, LEA, Political, and External actions, and those which comprise Reputational Attacks on the system. These risks are listed in Column B of the attached spreadsheet. We have guesstimated the likelihood of each of these *sources* of risk contributing to a system failure (factor A) in Column C.

Several Recommendations (i) for researchers, (ii) for LEAs, are introduced at the end.

2. Introduction

2.1. Background

This Deliverable is focused on incidental findings and residual risks, to set a policy for the SPIRIT project. Before completing this Deliverable, several actions were previously taken. These actions included:

- A risk analysis and a Data Protection Impact Assessment (DPIA) prior to the start of the project (see Annex 1)
- A risk management policy to respond to the risks identified in the DPIA
- A strategy for internal and external monitoring of ethical and legal aspects
- A Data Protection by Design (DPbD) strategy, i.e. a specific ontology (privacy-preserving software) to be embedded into the system
- A specific regulatory strategy to monitor, control and rule the processing information flows (the construction of the SPIRIT regulatory model)
- A differentiation between mock-up and real data to be processed (the project will use mock-up and synthetic data previously anonymised by the EU VALCRI project[1]; real data will be only managed by police departments at the testing stage)
- Service Contracts with all the police forces involved to clarify the level of access to public data as well as the conditions to access the project results

[1] Visual Analytics for Sense-making in CRiminal Intelligence analysis (VALCRI), https://cordis.europa.eu/project/rcn/188614_en.html

Project funded by H2020 Programme – Grant Agreement number: 786993

- A letter of commitment, agreeing not to sell the results of the project to nondemocratic countries
- A preliminary policy for managing potential re-identification issues, addressing risks of misuse of personal data
- A first set of measures for the reduction of residual risks and incidental findings

We follow up in this Deliverable the incidental findings policy, linking it with a revision of the DPIA and residual risks. After a close examination, we turn incidental findings into incidental risks, to strengthen and reduce them as much as possible. The outcome is a manageable matrix and a related set of guidelines (i) for the SPIRIT Project (ii) and for the fair use of the resulting platform. Incidental findings are usually defined as a kind of negative serendipity. i.e. findings that can unexpectedly come up from a research, exploratory, diagnostic or investigative process with a potential capacity to cause harm. By residual risks we mean the remaining risks after controls have been implemented and monitored, and the effect of their findings considered. Yet, we will keep using the former use of the notion, when needed.

2.2. Incidental findings

The notion of incidental findings originated in medical and genetic research.[2] Hence, it is a bio-ethical notion applicable to physical diagnosis, radiology, and brain image exploration (MRI) (Wolf et al. 2008). In what follows we describe these bio-ethical concepts briefly and then apply them to the notions of privacy and personal safety required for the current investigation. There are some differences too between the operability of the notion in medical and genetic research.[3]

[2] According to Damjanovicova (2016: 90) incidental findings became an issue within genomic medicine in the transition from targeted genetic testing to genome-scale screening testing. Targeted genetic testing consisted of probes, which targeted particular sequences in the genome known to be linked to diseases for which the test was performed.

[3] "Biobank research and rapidly increasing studies in genomics, proteomics, and nutrigenomics continue to identify many genes and biomarkers associated with risk of disease. Genetic testing for monogenic disorders are well established in health services, but little is yet known of the best way to handle complex risk information associated with multifactorial disorders in which the predictive importance of individual elements – genetic, epigenetic, or environmental – will differ for different individuals. The value of being informed about an incidentally discovered genetic risk (be it inherited or caused by a virus) is therefore much more difficult to ascertain than that for an incidentally discovered pathogenic condition revealed, for example, in a brain imaging study." (Viberg et al. 2014)

In a broad sense incidental finding include both false positives and marginal findings with no clinical relevance occurring within doctor-patient relationships. In a narrower sense, (i) they occur in participants during a scientific study, (ii) they potentially might affect the health or reproductive capacity of participants, (iii) they were not intended in the study's aim (Schmücker, 2016). Erdmann (2016) differentiates (i) incidental findings, (ii) secondary findings (as a result of the first ones), and (iii) discovery findings. The handling of "incidentalomas" (abnormalities revealed during imaging, which were not accompanied by any symptoms) raise ethical concerns in all three cases, although the influential report *Anticipate and Communicate. Ethical Management of Incidental and Secondary Findings in the Clinical, Research, and Direct-to-Consumer Contex*t published by the Presidential Commission for the Study of Bioethical Issues (USA Presidential Commission) in December 2013 treats only incidental and secondary findings. We will come back into this later (Section 6).

Damjanovicova (2016) summarises the most pressing ethical questions in the debate on the management of incidental findings as it pertains to medical research as follows:

• should the physician be obligated to report all such findings back to the patients, or just some findings—in that case, which ones, or none?
• should the patients have a right to demand such results to be delivered to them under all circumstances, or should they be allowed to refuse to receive any such information?
• should a patient with a genetic variant implicated in the development of serious, but preventable/treatable clinical condition be allowed to refuse to know such information and consequently withhold it from family members that can also be carriers of that same genetic variant?
• should some genetic variants that can cause preventable/treatable clinical conditions that come up as incidental results in genome-scale screening testing as be actively sought in such testing, becoming thus a secondary instead of incidental finding, or, in fact, a regular finding of the clinical screening?

Bunnick et al. (2017) characterizes detection and feedback of incidental findings as a "double edged sword", as they may allow for timely treatment and thus lead to medical benefit but may also harm research participants because of the burdens of costs of follow-up testing and (possible) over-treatment. Thus, their disclosure raises an ethical dilemma: to refer for further work-up or to remain silent. The authors propose a seven-step framework and minimum requirements for pathways for their detection, management and communication in large-scale imaging studies. It includes: (i) anticipation of incidental findings (lists); (ii) information provision and informed consent of the research participants (research participants should be given should be given the opportunity either to opt out of receiving information about incidental findings or to withdraw from the study); (iii) radiographers should be instructed whether and to what extent to review scans for abnormalities during scan acquisition; (iv) some form of routine review of research scans should be arranged; (v)

Project funded by H2020 Programme – Grant Agreement number: 786993

detected abnormalities should be confirmed by experts (i.e. radiologists) before they are reported to the research participants; (vi) communication of the incidental finding policies to the research participant should align with national regulations and customs; (vii) researchers should take responsibility for the clinical follow-up of the research participant (i.e. through adequate and timely referral).

2.3 Adjustment to security and policing scenarios

Bioethical studies constitute a good standpoint from which to address ethical concerns. We can benefit from their results to start thinking about security and policing, because they embrace *a relational and contextual perspective*. I.e. they consider the overall relation between all participants: doctors, researchers, patients, and the situation of third parties affected.

However, a direct translation or projection to the security field requires some adjustments, due to the informational processing character of the risks and the potential harm caused to the rights and everyday life of citizens. As already stated in our previous answer to the Ethical Commission[4], identity management, privacy and data protection, and the possibility of social and political discrimination raise more issues that parallel but do not equate to the possible harms in biological, genetic, and medical sciences. Some more constraints apply in the scenarios created in security and policing environments because of the imbalance of power between the different stakeholders. I.e. LEAs are usually compliant with internal and external best practices, regulations and legislation. They are supposed to follow appropriate procedures, and it is generally the case that they do so. But incidental policy guidelines should reflect all possible harms, including those caused by intentional behaviour (for instance, vendettas, bribery and conflicted personalities). The analysis of hazards should include as many cases as possible to be useful to internal and external controllers and minimise the risks. This is another way of stating that (i) compliance with laws, regulations and court assessments, (ii) technological conformance with existing standards, (iii) and congruence with ethical principles, could be better achieved if based on empirical knowledge and reasonable estimation.

Recommendation CM/Rec (2017) 6 of the Committee of Ministers to member States on "special investigation techniques" in relation to serious crimes including acts of terrorism takes a proportioned approach, in which security is not bartered against privacy, but balanced, as the principles of General Data Protection Regulation as well as of the Police and Justice Authorities Directive (2016/680/EU) also apply to LEA's behaviour in investigative matters. The Recommendation is mindful of "the obligation on member States to maintain a fair balance between ensuring public safety through law

[4] SPIRIT. *Reply to the Ethics Second Assessment Report*, April 30th 2018, section 9.3.3.

enforcement measures and securing the rights of individuals, as enshrined in the provisions of the European Convention on Human Rights and the case law of the European Court of Human Rights in particular". Articles 7-10 list the protections to be considered:

> 7. Special investigation techniques should only be used where there is sufficient reason to believe that a serious crime has been committed or prepared, or is being prepared, by one or more particular persons or an as-yet-unidentified individual or group of individuals.
>
> 8. Member States should ensure proportionality between the special investigation techniques used and the legitimate aims pursued. In this respect, when deciding on their use, an evaluation in the light of the seriousness of the offence and the intrusive nature of the specific special investigation technique used, should be made. Also the urgency and general complexity of the case could be considered.
>
> 9. Member States should ensure that competent authorities apply less intrusive investigation methods than special investigation techniques if such methods enable the offence to be prevented, detected, investigated, prosecuted and supressed with adequate effectiveness.
>
> 10. Member States should take appropriate legislative measures to permit the production of evidence gained from the lawful use of special investigation techniques before courts. Procedural rules governing the production and admissibility of such evidence shall safeguard the rights of the accused to a fair trial.

The recent *EU Practical guide on the use of personal data in the police sector* (2018: 9) reads:

> If data processing is likely to result in a high risk to the individual's rights, the data controller should perform a Data Protection Impact Assessment (DPIA) to assess all risks for the envisaged actions. Considering that the introduction of new data processing technologies bears *per se* such potential risk, it is likely that the introduction of such new technology will make a DPIA advisable. It is recommended that the assessment of risk is not static, but takes into account the specific case, it is repeated at reasonable intervals, and that it touches upon relevant phases of the data processing activity and that it takes into account accountability considerations. It is also of great importance, that in terms of data security and safety of communications, the highest standard is taken into account when introducing such technologies.
>
> Example: New data mining techniques may offer extended possibilities for identification of possible suspects and should be assessed carefully for their compliance with existing data protection law, together with assessment of the risks it may represent to individual's rights and suggestions for the adoption of safeguards to ensure the protection of data, including with regard to data security.

This is certainly the case for SPIRIT. Thus, to set an incidental findings policy, we adopt a broad approach, also focusing on the remaining possible residual risks.[5] As already stated, in computer science and security contexts, the incidental findings subject has been incorporated recently, following the risks of disclosure of information and false positives produced in the context of Open Source Intelligence (OSINT) (Casanovas, 2017). This also include policing, which has been reported as "the incidental effects on policing" in law enforcement (Stoughton, 2014a).[6]

Law enforcement is a sensitive issue, leaning on the interaction between legal scholars' conceptual work, legal interpretation, case-law based decisions, and LEA practices. From a constitutional perspective, Stoughton puts it in the following way, elaborating on some USA Superior Court rulings pertaining to policing (2014b):

> Yet the majority of the Court factual assertions are made entirely without support or citation, raising concerns about whether the Court is acting based on a complete and accurate perception. When it comes to policing facts, the Court too often gets it wrong. […] Misunderstandings about law enforcement have led to constitutional rules that fail to align with the world that they were designed to regulate.[…] When constitutional rules are predicated on empirical information, a more accurate understanding of police practices will better align those rules with reality leading to both more precise constitutional rule making and more efficacious liberty protections.

The same author formulates a relevant question: "How, then, can we best ensure that officers engage in good policing, given the wide variety of tasks they must perform?" (Stoughton, 2016: 612). He advocates that "a more fundamental reform is necessary: the core principles of policing need to be adjusted to change how officers view their job and their relationship with the community." Education certainly plays a role. So do instruction and training. But to "build public trust and increase police legitimacy" (ibid.) all solutions require a better knowledge of facts, a better legal coordination with police practices (including police cooperation), and a reliable description of all the issues at stake.

[5] SPIRIT. *Reply to the Ethics Second Assessment Report*, April 30st 2018, section 9.3.3.

[6] "When I refer to the incidental regulatory effects of policing neutral law, I mean the unintended but often profound ways that certain laws, which happen to include police within a broader regulatory ambit, change officer behaviors in ways that are unintended and often entirely unexpected." (Stoughton, 2014: 2185-86). This includes several regulations not directly addressed to LEAs, as "they are also employers, government agencies, and, for the most part, entities organized at the city or county level. As such, they are subject to laws that happen to include police agencies as constituents of a broader regulatory ambit." (ibid. 2196).

2.4. Residual risks

In this Deliverable, we follow the classical approach of drawing a risk matrix for hazards, but we also consider more recent developments. Consequence and probability categories give the axes of a co-ordinate system (Gheorghe and Mock, 1999). We reproduce their list of definitions of consequence and probability categories (tables 1 and 2, ibid: 69-70).

Table 1. Hazard severe categories.

Description	Category	Definition
Catastrophic	I	Death, system loss, or severe environmental damage
Critical	II	Severe injury, severe occupational illness, major system or environmental damage
Marginal	III	Minor injury, minor occupational illness, or minor system or environmental damage.
Negligible	IV	Less than minor injury, occupational illness, or less than minor system or environmental damage.

Table 2. Hazard probability levels

Description	Level	Specific Individual Item	Fleet or Inventory
Frequent	A	Likely to occur frequently	Continuously experienced
Probable	B	Will occur several times in the life of an item	Will occur frequently
Occasional	C	Likely to occur some time in the life of an item	Will occur several times
Remote	D	Unlikely but possible to occur in the life of an item	Unlikely but can reasonably be expected to occur
Unprobable	E	So unlikely, it can be assumed occurrence may not be	Unlikely to occur, but possible experienced

Matrices present a degree of subjectivity, that we try to control when assigning probabilities, which present a subjective or interpretative dimension. There also are common fallacies relating to the issue

of avoiding unreasonable judgments of risk. Johnsen et al. (2017) contends that a safety culture should be developed with countermeasures to the common fallacies in risk perception, not addressed by functional safety standards. Planning a continuous residual risks reduction may contribute to stabilising such a culture, aligned with smart governance principles. Zero tolerance is a government policy applied to eliminate harassment, violence, illegal narcotics, driving under the influence of alcohol, and illegal weapons. Thus, safety should be aligned with security and privacy.

Safety is a dynamic control problem. "Human error is a symptom of a system that needs to be redesigned", instead of "prevent failures" we should "enforce safety constraints on system behaviour" (Leveson, 2011, 2013). In the last economic crisis, the financial system did not adequately control the use of financial instruments. Leveson differentiates safety from security. Safety "prevent[s] losses due to unintentional actions by benevolent actors", security "prevent[s] losses due to intentional actions by malevolent actors". The common goal is loss prevention: (i) to ensure that critical functions and services provided by networks and services are maintained; (ii) demonstrating that an integrated approach to safety and security is possible; and (iii) showing that a paradigm for safety that can work for security too. Leveson contends that this integration can be produced through a top-down system engineering approach.

In keeping with this later assessment, we will adopt not only a top down, but also a *middle-out approach*, in which social engineering can be combined with systemic measures to monitor and control both the system, the human beings involved in its management, and the framework in which hazards occur and residual risks remain. Young and Levenson (2013) extends Levenson's STPA (Systems-Theoretic Process Analysis) to security, STPA-SEC. They reframe the security approach based on guarding against cyber-attacks into a socio-technical perspective focusing on vulnerabilities that allow disruptions to propagate throughout the system.[7] This would reduce risks to residual risks. But even though, as stated by the overall view of risk management by Havinga and Sessink (2016), chance and damage are uncertain in IT security for four main reasons: (i) vulnerabilities change frequently[8], (ii) the IT environment itself changes continuously, which changes both the probability

[7] According to Young and Levenson (2013) there are four types of potential unsafe/unsecure control actions: (i) providing a control action leads to a hazard or exploits the vulnerability; (ii) not providing a control action leads to a hazard or exploits a vulnerability; (iii) providing control actions too late, too early, or in the wrong order leads to a hazard or exploits a vulnerability; (iv) stopping a control action too soon or continuing it too long leads to a hazard or exploits a vulnerability.

[8] For instance, "at a certain moment, for example, it may seem impossible to gain unauthorized access to a system, a week later there may be a zero-day exploit and an experienced hacker may gain access, one week later an exploit is released on the internet and access is possible for every "script kiddy", and again one week later the vulnerability is patched and unauthorized access seems impossible again." (Havinga and Sessink, ibid. 2018)

and the potential damage, (iii) the chance that a threat causes damage is influenced by unknown external factors, and (iv) the cost of the damage is hard to estimate.

In the following sections, we enhance the preliminary results of the SPIRIT DPIA (See Annex 1) to identify vulnerabilities and propose an extended incidental findings policy associated with an improved residual risks analysis.

3. A Model for Evaluating Incidental and Residual Risks for the SPIRIT project

3.1. DPIA Preliminary Results and Risk Mitigation

In our *Reply to the Ethics Second Assessment Report* (April 30th 2018, section 9.3.3), we came to the following preliminary conclusions (number references are reported in Annex 2):

1. Risks related to the lawfulness of the overall process have been sufficiently mitigated, as the relevant legal issues have been identified and foreseen in advance (1-4).

2. Risks related to purpose specification have been sufficiently mitigated, as data will be collected for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes. Close monitoring of the activities involving real data will be conducted throughout the duration of the project (5-9).

3. Risks related to data minimisation have been identified, but are not completely mitigated. Therefore, further measures will need to be implemented (10-17).

4. Risks related to data accuracy have been identified, but are not completely mitigated. Therefore, further measures will need to be implemented (18-24).

5. Risks related to data security have been sufficiently mitigated, (i) as technical partners have set anonymization and encryption measures, (ii) actions will be taken in case of data breaches, (iii) individuals will be duly informed if their personal data is lost, stolen or other compromised, (iv) each end-user is deemed to act as controller, and (v) the Ethical lead will be in permanent contact with the EAB. Close monitoring of the activities involving real data will be conducted throughout the duration of the project (25-31).

6. Risks related to access rights have been sufficiently mitigated, as access rights of participants in the research will be exercised before the coordination of the Consortium and access rights of individuals whose data are contained in LEA data sets or processed by LEAs in the evaluation phase before the

relevant LEA. Individuals will be provided with the possibility to access and correct their personal information, and ask for correction and deletion, unless it is not legally possible according to the limitations included in Article 15 of Directive 2016/680. (32-35). 61

7. Risks related to accountability have been identified, but not completely mitigated. Further measures will need to be implemented. The potential misuse of the research requires a special attention as it might generate residual and incidental risks. This will be closely followed and monitored by the SPIRIT ethical lead and the Independent Ethical Board, according to the provisions of the SPIRIT regulatory model. Oversight mechanisms to overview existing practices and to provide guidance to the partners of the Consortium will be put in place (37-42).

3.2 Evaluating Incidental and Residual Risks

In the light of the approach of identifying vulnerabilities as much as possible, we now describe the operation of a spreadsheet-based model which seeks to calculate the overall risks which may be faced by the SPIRIT system, both before and after policies have been implemented to mitigate these risks. The model has yet to be calibrated using data on each of the risks – a process which will require considerable resources and time – but in order to illustrate the working of the model, we have populated it with example, very preliminary, guesstimates.

We define *incidental risks* as the risks of misuse of the system caused by internal and external factors. These risks can be mitigated (reduced) by the use of suitable *policies*. The risks that remain after these policies have been implemented and taken full effect are termed *residual risks*.

In order to identify possible sources of incidental risks we have reviewed privacy and data protection inquiries, press coverage, and the academic literature on the subject. This investigation has focused particularly on the recent literature and experience following the introduction of new European data protection regulations, the General Data Protection Regulation (GDPR, 2016), enacted on May 25th, 2018 [9], and especially in this matter the Police and Justice Authorities Directive (2016/680/EU).[10]

Recital (52) of the Directive 2016/680 reads:

> The likelihood and severity of the risk should be determined by reference to the nature, scope, context and purposes of the processing. Risk should be evaluated on the basis of an objective assessment,

[9] https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng
[10] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0680&from=EN

through which it is established whether data-processing operations involve a high risk. A high risk is a particular risk of prejudice to the rights and freedoms of data subjects.

We have grouped the incidental risks into five *sources* – those emanating from Individual, LEA, Political, and External actions, and those which comprise Reputational Attacks on the system. These risks are listed in Column B of the attached spreadsheet. We have guesstimated the likelihood of each of these *sources* of risk contributing to a system failure (factor A) in Column C.

For each of the *categories* of risk identified, for each of the sources of risk, we have then guesstimated the likely incidence of a system failure occurring. For the present, we have three levels of severity (factor B - shown in column D) - high (H), medium (M) and low (L), to which we allocate a preliminary incidence of 30%, 20% and 10% respectively. A weight is also applied to each category for each source, indicating the importance of that category in the overall probability of the relevant source causing a failure (factor C - shown in column E).

Cross-multiplying A*B*C gives us a combined probability of the risk category eventuating in a system failure. Adding the probabilities across all sources gives us an overall probability of a risk occurring from all sources and categories. The result is to be found in cell F40 in the attached spreadsheet.

Column G identifies some of the data sources which will be needed to calibrate the model and to turn our guesstimates into something more robust.

Column H provides a partial list of the policies which could be employed to mitigate the risks. We emphasise that this list is also very preliminary and will need to be refined before the model can be used for policy guidance.

In column I, we have guesstimated the effect on the overall incidental risk emanating from each source that each policy might be expected to have. Column J then calculates the residual risk that remains once these mitigating effects have been taken into account. The overall result may be found in cell J40.

Using our, very preliminary, settings for the model we estimate the pre-policy incidental risks to be 22.9% - that is if no effort is taken to mitigate the various risks, there could be a probability of failure of 22.9% - and the policies suggested in column H might be expected to reduce this risk to a residual 6.2%.

Obviously, the objective of the policies is to create zero residual risk, and hopefully the data can be validated, and the policies refined so that this outcome – or something very close to it - is achieved. We have plotted in Figure 1 a general model visualisation. We have aligned in Figures (2-11) sources

of risk and corresponding mitigation policies for individuals, LEAs, politics, external, and reputational.

Fig. 1. Visualisation of the Model for Evaluating Incidental and Residual Risks

European Commission | Horizon 2020 European Union funding for Research & Innovation

Project funded by H2020 Programme – Grant Agreement number: 786993

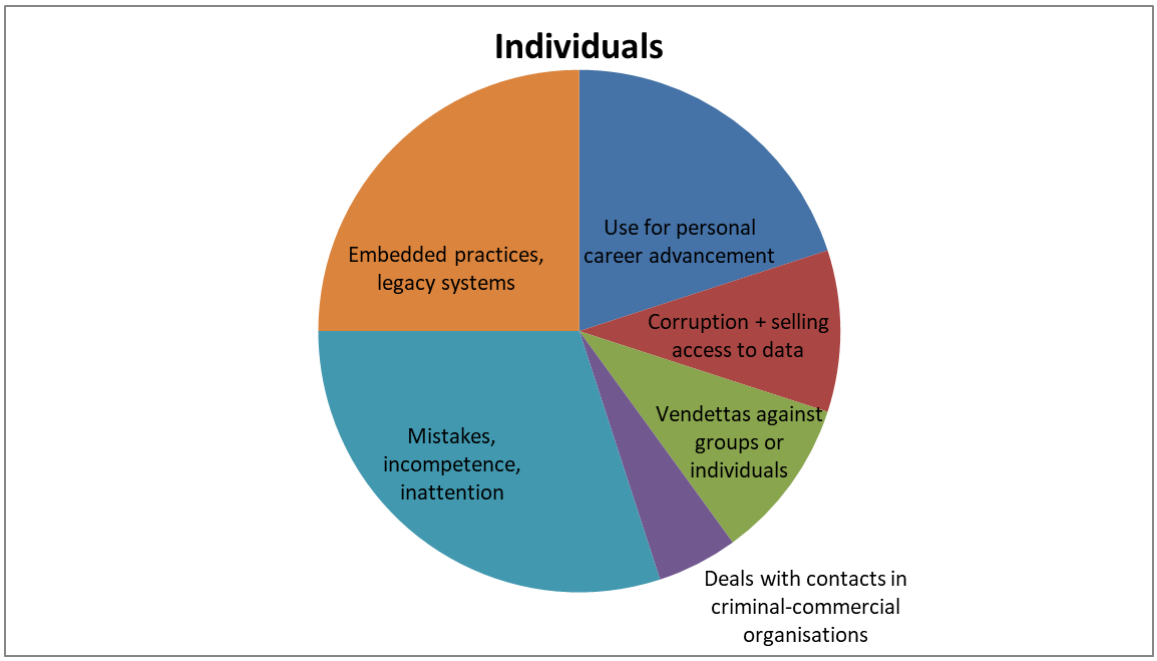


Fig. 2. Source of risks: Individuals

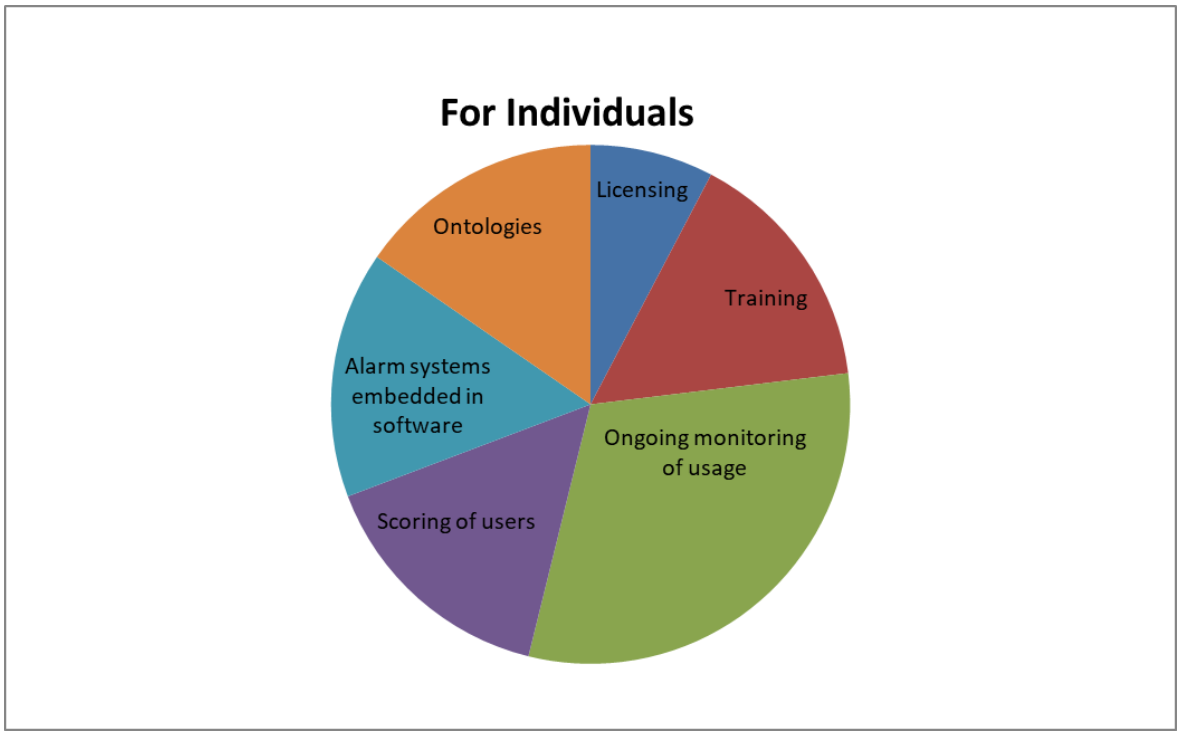


Fig. 3. Mitigation policy: Individuals

European Commission | Horizon 2020 European Union funding for Research & Innovation

Project funded by H2020 Programme – Grant Agreement number: 786993

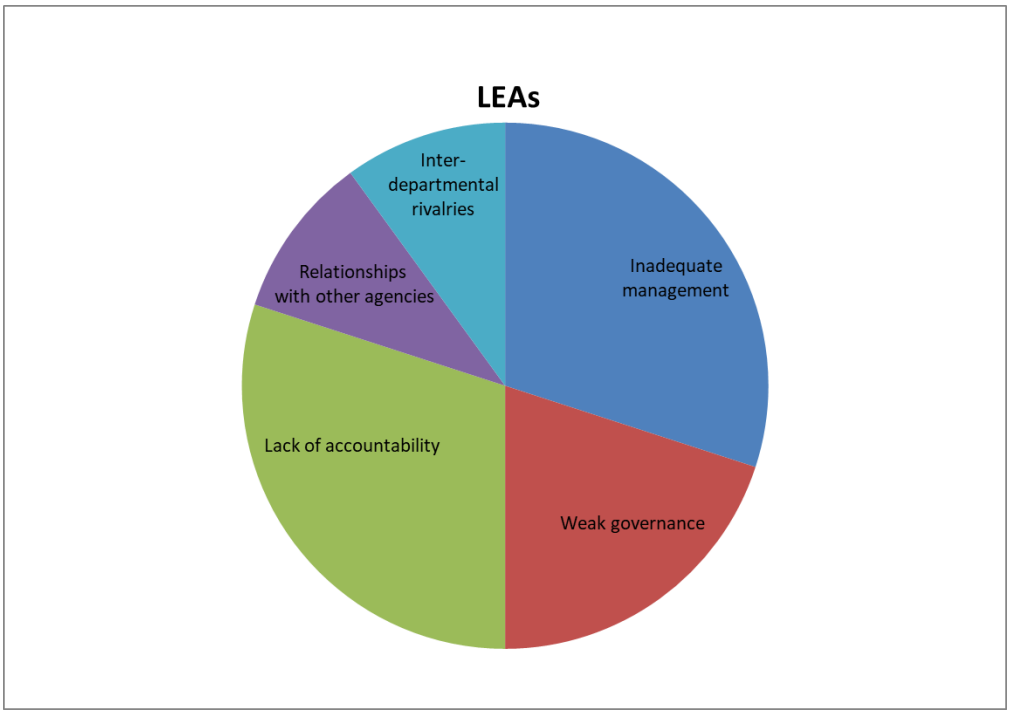


Fig.5. Source of risks: LEAs

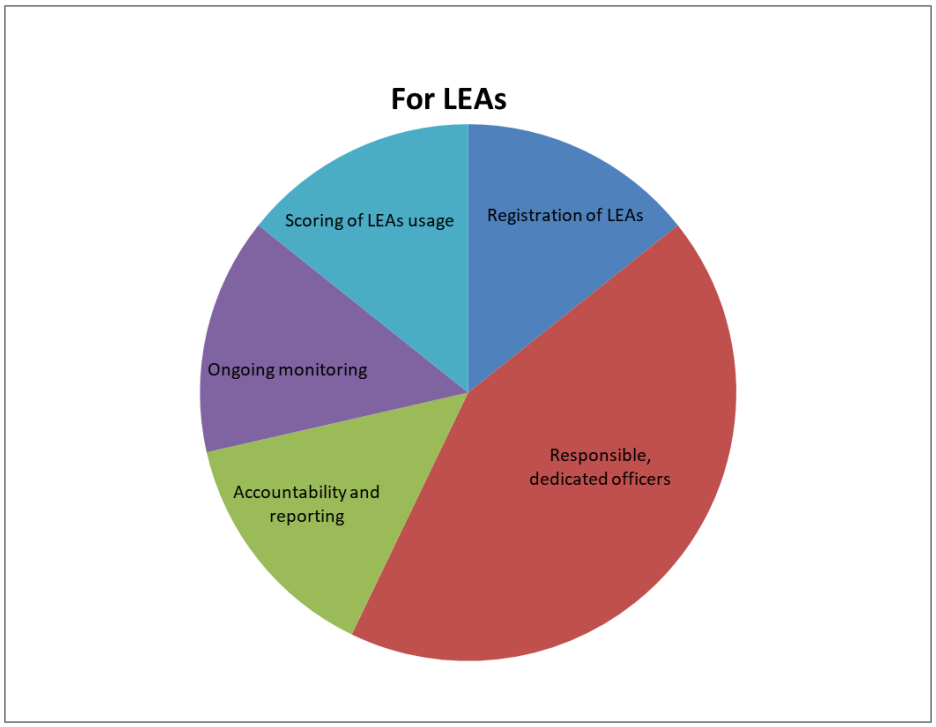


Fig.6. Mitigation policies: LEAs

European Commission | Horizon 2020 European Union funding for Research & Innovation

Project funded by H2020 Programme – Grant Agreement number: 786993

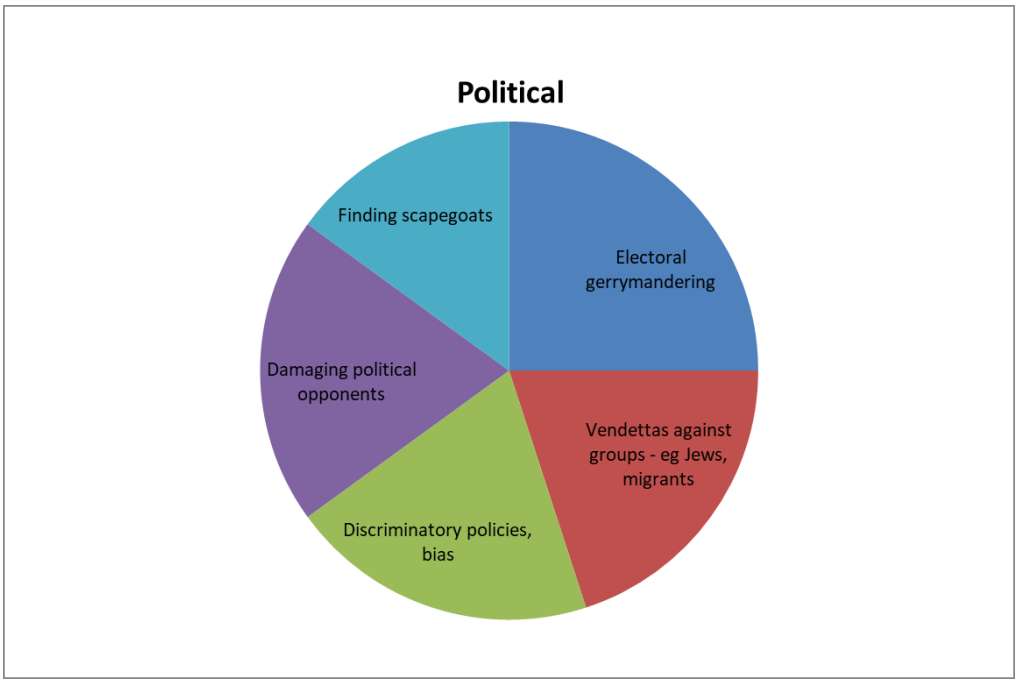


Fig. 7. Source of risk: Political

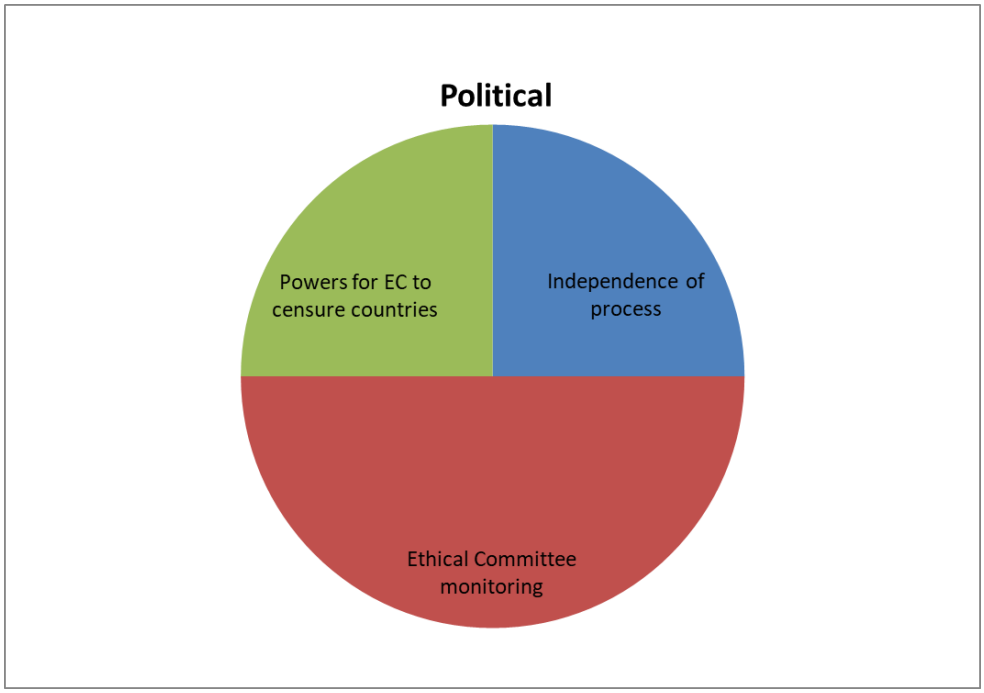


Fig. 8. Mitigation policy: Political

European Commission | Horizon 2020 European Union funding for Research & Innovation

Project funded by H2020 Programme – Grant Agreement number: 786993

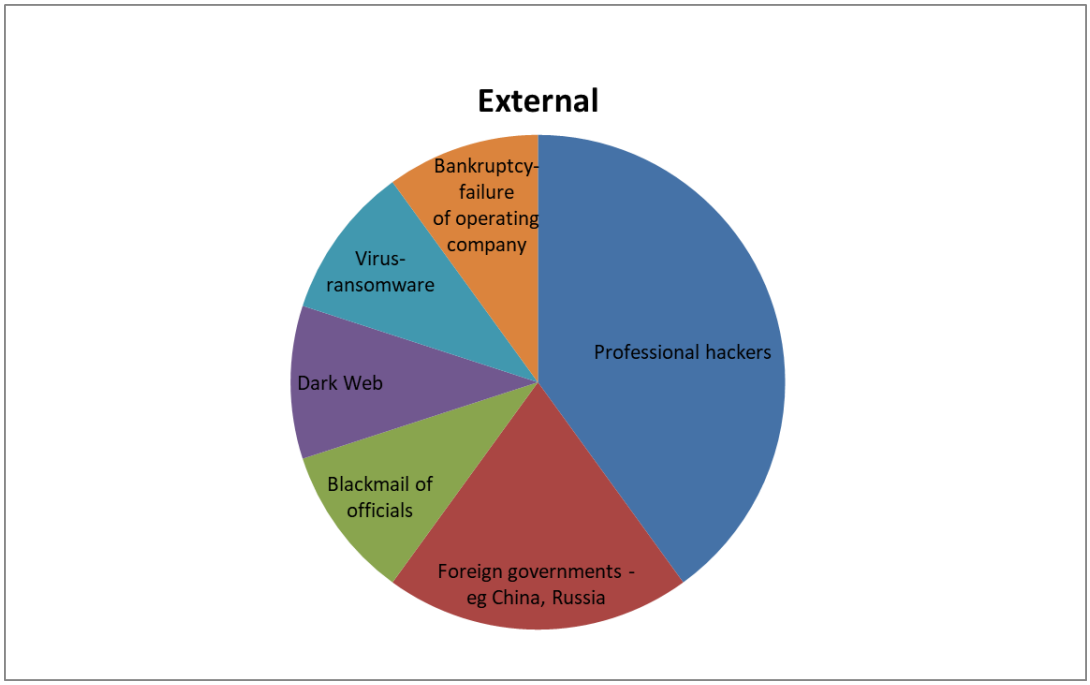


Fig. 9. Source of risk: External

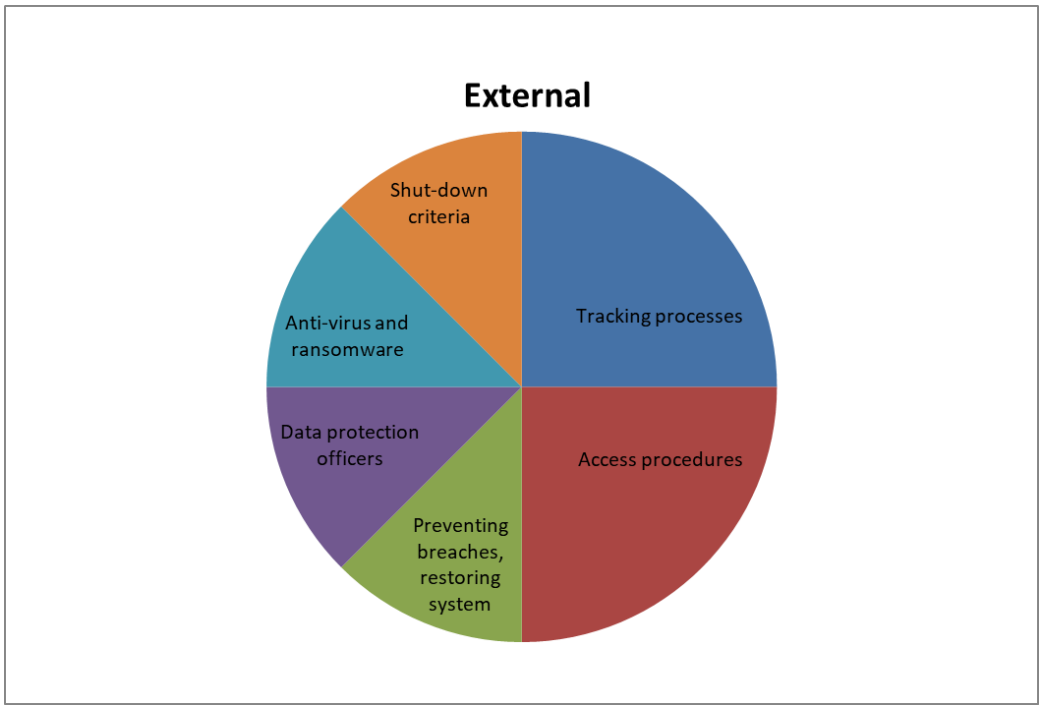


Fig. 10. Mitigation policy: External

European Commission | Horizon 2020 European Union funding for Research & Innovation

Project funded by H2020 Programme – Grant Agreement number: 786993

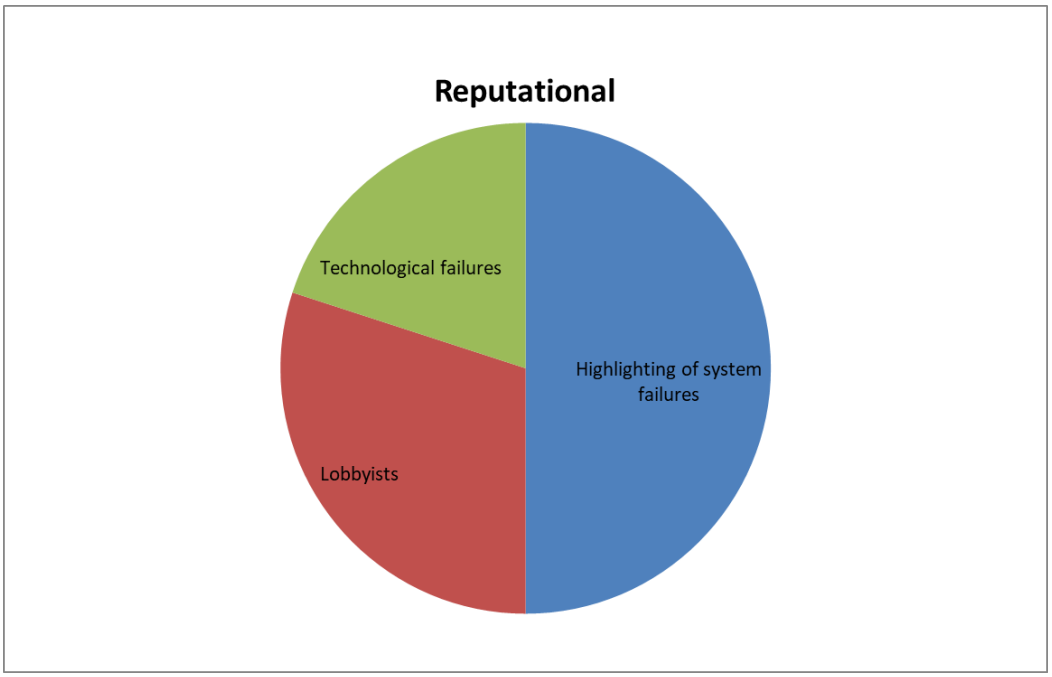


Fig. 11. Source of risk: Reputational

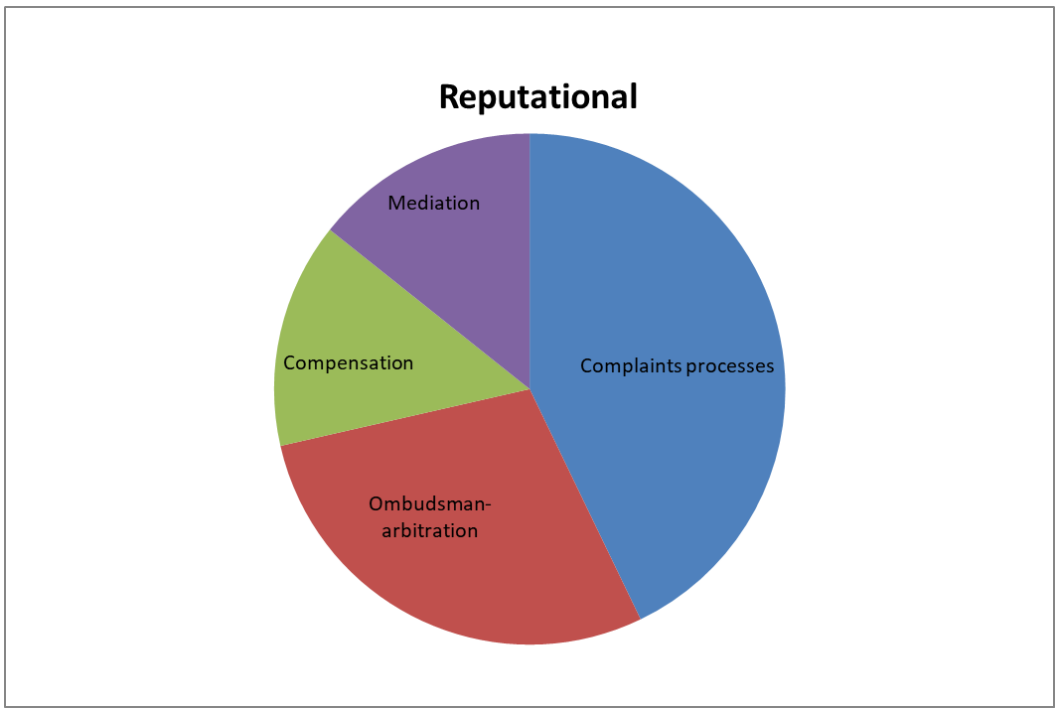


Fig. 12. Mitigation policy: Reputational

European Commission | Horizon 2020 European Union funding for Research & Innovation

Project funded by H2020 Programme – Grant Agreement number: 786993

3.3 Matrix

Incidental Risk Analysis			Preliminary Scoring		
		A	B	C	A*B*C
Source of Risk	Categories	Source likelihood (%)	Likely incidence of risk category (H, M, L)	Weight (as % source)	Risk Incidence
Individuals	Use for personal career advancement	30	H	20	1.8%
	Corruption + selling access to data		H	10	0.9%
	Vendettas against groups or individuals		H	10	0.9%
	Deals with contacts in criminal-commercial organisations		H	5	0.5%
	Mistakes, incompetence, inattention		H	30	2.7%
	Embedded practices, legacy systems		M	25	1.5%
				Total	**8.3%**
LEAs	Inadequate management	10	H	30	0.9%
	Weak governance		H	20	0.6%
	Lack of accountability		H	30	0.9%
	Relationships with other agencies		M	10	0.2%
	Inter-departmental rivalries		M	10	0.2%
				Total	**2.8%**
Political	Electoral gerrymandering	20	M	25	0.5%
	Vendettas against groups - eg Jews, migrants		H	20	0.6%
	Discriminatory policies, bias		M	20	0.4%
	Damaging political opponents		M	20	0.4%
	Finding scapegoats		M	15	0.3%
				Total	**2.2%**
External	Professional hackers	30	H	40	3.6%
	Foreign governments - eg China, Russia		H	20	1.8%
	Blackmail of officials		M	10	0.6%
	Dark Web		M	10	0.6%
	Virus-ransomware		H	10	0.9%
	Bankruptcy-failure of operating company		M	10	0.6%
				Total	**8.1%**
Reputational attacks	Highlighting of system failures	10	M	50	1.0%
(by press etc?)	Lobbyists		L	30	0.3%
	Technological failures		L	20	0.2%
Total		**100**		**Total**	**1.5%**
				Overall	**22.9%**
			H	30%	
			M	20%	
			L	10%	
			As % opportunity		

European Commission | Horizon 2020 European Union funding for Research & Innovation

Project funded by H2020 Programme – Grant Agreement number: 786993

		Development of Mitigation Policies			
Source of Risk	**Categories**	**Data sources to identify possible prevalence**	**Policies to reduce risks and their impact**	**Mitigation effect (% reduction in overall source risk)**	**Residual risk**
Individuals	Use for personal career advancement	Salary and bonus data	Licensing	5	
	Corruption + selling access to data	Press reporting of past events	Training	10	
	Vendettas against groups or individuals	Complaints against LEAs	Ongoing monitoring of usage	20	
	Deals with contacts in criminal-commercial organisations		Scoring of users	10	
	Mistakes, incompetence, inattention	Previous inquiries into LEAs	Alarm systems embedded in software	10	
	Embedded practices, legacy systems		Ontologies	10	
			Total for source	**65**	**2.9%**
LEAs	Inadequate management	Inquiries into LEAs	Registration of LEAs	10	
	Weak governance	Annual reports	Responsible, dedicated officers	30	
	Lack of accountability	Reporting processes	Accountability and reporting	10	
	Relationships with other agencies	Internal government reports	Ongoing monitoring	10	
	Inter-departmental rivalries		Scoring of LEAs usage	10	
			Total for source	**70**	**0.8%**
Political	Electoral gerrymandering	Press coverage of previous behaviour	Independence of process	20	
	Vendettas against groups - eg Jews, migrants	Complaints	Ethical Committee monitoring	40	
	Discriminatory policies, bias		Powers for EC to censure countries	20	
	Damaging political opponents	Survey data			
	Finding scapegoats	Case studies			
			Total for source	**80**	**0.4%**
External	Professional hackers	Vulnerability assessments	Tracking processes	20	
	Foreign governments - eg China, Russia	Risk assessment by security services	Access procedures	20	
	Blackmail of officials		Preventing breaches, restoring system	10	
	Dark Web	Reports of DW activity	Data protection officers	10	
	Virus-ransomware	Techical assessment of current threats	Anti-virus and ransomware	10	
	Bankruptcy-failure of operating company	Due diligence on company	Shut-down criteria	10	
			Total for source	**80**	**1.6%**
Reputational attacks	Highlighting of system failures	Past press reports on government syste	Complaints processes	30	
(by press etc?)	Lobbyists	Surveys of public officials	Ombudsman-arbitration	20	
	Technological failures	Technical assessment of robustness	Compensation	10	
			Mediation	10	
Total			**Total for source**	**70**	**-0.8%**
					5.0%

4 SPIRIT Incidental Findings Policies

4.1 Incidental policies in the SPIRIT Project

Within the SPIRIT Project we distinguish between (i) incidental findings that may occur during research, and (ii) incidental findings that may occur in the use of the technology by LEAs. The later ones can have an impact on the rights of individuals whose data have been collected during an investigation and might not have any involvement in that investigation.

Incidental findings in the context of the SPIRIT project can be understood as follows:

1. The potential discovery of patterns within synthetic data of the mock up social networks which do not appertain to any real person so will not need to be addressed as an incidental finding in the normal sense of the concept.

2. Incidental Findings within the LEA environment which may relate to pattern discovery under the regulated police investigatory processes, either to eliminate persons from any association with criminal activity or to help/confirm/disconfirm any hypotheses regarding some aspect of the organised crime being investigated. Thus, essentially LEAs will have specific mandatory regulations about how dealing with incidental discoveries (under any category where personal data disclosure to the data subject should be performed or avoided).

3. Incidental findings related to the unlikely but nonetheless possible relevance of this issue to any interactions that the project team may hold with invited participants. Such an involvement necessarily entails the implementation of a full consent process. In such Consent Seeking Process, the prospective participants will be informed, among other requisite information, of the Incidental Finding Policy of the project.

4. Incidental findings as incidental risks, as described in sections 3.2. and 3.3.

Points (1-3) is a narrow way of understanding findings, closer to the original meaning of the concept. Point 4 relates to the matrix drawn. We'll treat these policies separately.

4.2 Policy for re-identified data

Within the SPIRIT project, research will be undertaken using different datasets, including ad hoc created mock-up data as well as anonymised data from West Midlands Police. This last data set was constructed by A E Solutions (AES) during the EU funded Valcri project and is fit for use within the SPIRIT project.

As detected in the DPIA (see section 9), when using such data there may be the possibility of reconstructing the information to identify a real person thus incurring in re-identification. This type of risk will be managed by the policy represented in the flowchart illustrated in Figure 13.

The figure shows the flow of potential results and decisions that may occur at each stage when using one or more of the anonymised data sets to develop and test one or more algorithms.

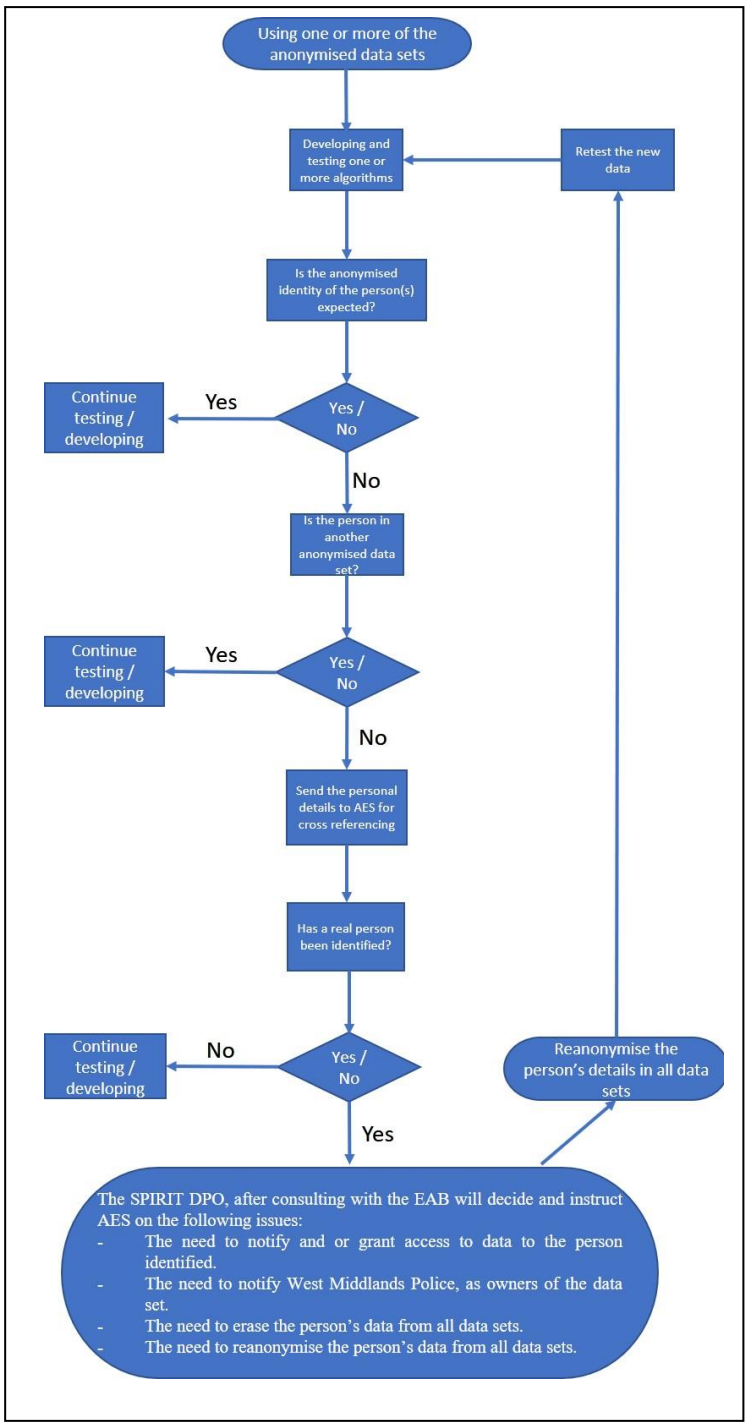


Fig. 13. SPIRIT policy for data re-identification risks

The figure shows the flow of potential results and decisions that may occur at each stage when using one or more of the anonymised data sets to develop and test one or more algorithms.

In particular the flowchart shows the potential results when using one or more of the anonymised data sets. Let's imagine, using the flowchart, that the researcher/developer is developing and/or testing an algorithm with a query on an investigation in which Gordon Smith is the anonymized name of a person of interest. During the development or testing of an algorithm, has the result that has been returned provided the name Gordon Smith? If so, continue testing. If that name has not been returned, has the result provided another anonymized name? The name that has been returned can be further validated by looking within the other anonymized data sets if required. This is acceptable as it has demonstrated that the result is in error and the algorithm requires further development, so the testing and development phase can continue. If the name that is returned does not appear in any of the anonymized data sets this may indicate that a real person may have been identified. This information will be sent to AES for cross-referencing. If the name does not relate

to a real person, the testing/developing can be continued. In the event that a real person has been identified the policy foresees that the researcher/developer that detects the problem must immediately notify AES, as the partner responsible for anonymisation in the SPIRIT project, and the SPIRIT DPO.

The SPIRIT DPO, after consulting with the EAB will decide and instruct AES on the following issues: (i) the need to notify and/or grant access to data to the person identified; (ii) the need to notify West Midlands Police, as owners of the data set; (iii) the need to erase the person's data from all data sets; (iv) the need to re-anonymise the person's data from all data sets.

4.3. Privacy preserving algorithm development[11]

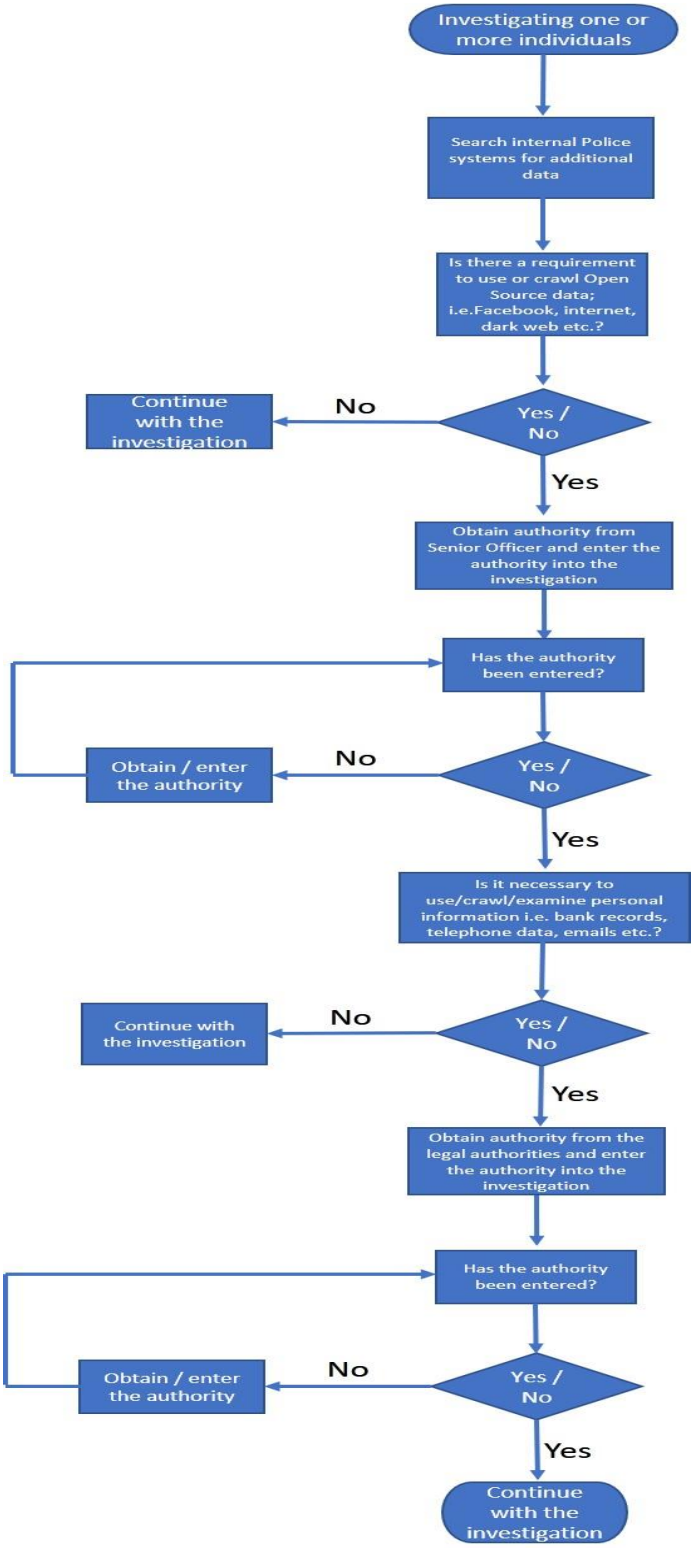
To ensure that the privacy of individuals is safeguarded- both during the validation and training phases and in the final technology resulting from SPIRIT- in the development phase, human intervention points will be built into algorithms, methods and crawlers so that, when used, it will provide transparent levels of authority to progress the investigation into open source data or closed data such as emails, closed social network profiles, bank records, etc.

Legislation differs in Member States on what type of personal data police forces are allowed to access, under which circumstances and through what procedures, although the EU Directive (EU) 2016/680 may harmonise it.[12] Police forces must strictly adhere to these requirements, and they do, as the risk is to have the criminal proceedings invalidated later on in court, due to the breach and the subsequent harm on the fundamental rights and freedoms of citizens.

The flow chart illustrated in Figure 14 represents the safeguards that will be included in the SPIRIT technological result to ensure the fundamental rights and freedoms of individuals. In particular there are two points in which police forces will have to enter into the investigation the relevant authorisations, either from a superior officer or from a judicial authority, according to the different legislations in the different countries. First, in those cases in which the legal provisions applicable to a LEA require an authorisation to include in the investigation open source data, and second, when there is a need to access information contained in private sources such as is the case for access to emails and other private sources. Most Member States require in these instances an authorisation from a judicial authority. These safeguards will be included in the SPIRIT system in the form of specific

[11] 4.3 and 4.5 reproduce the policy already presented in [11] SPIRIT. *Reply to the Ethics Second Assessment Report*, April 30th 2018, sections 6.1.2 and 6.1.3.

[12] Art. 63.1 sets the timeline: "Member States shall adopt and publish, by 6 May 2018, the laws, regulations and administrative provisions necessary to comply with this Directive. They shall forthwith notify to the Commission the text of those provisions. They shall apply those provisions from 6 May 2018."



technical measures that will not allow an investigation on the system to go further without introducing proof of the relevant authorisations.

Fig. 14. Privacy preserving algorithm development

4.4. Data Protection by design (DPbD): Ontology and SPIRIT Regulatory Model

As stated in the Reply[13], the SPIRIT indirect strategy to be developed along the Project entails the following action plan to mitigate the identified risks related to identity:

1. Defining the information flow in advance for all functionalities of the platform.
2. Embedding alerts and protections into the architecture to detect breaches and accidents as soon as possible, identifying the information flow in which the breach has been produced.
3. Defining and identifying ethical and legal requirements to be modelled, according to (i) hard law (national and EU regulations, GDPR,

[13] SPIRIT. Reply to the Ethics Second Assessment Report, April 31st 2018, section 9.

Directive 2016/680/EU), (ii) EU Data Protection Supervisor and national policies and Data Protection Authorities, (iii) soft law (protocols, standards), (iv) ethical expertise.

4. Introducing a quick communication system between researchers, LEAs, SPIRIT DPO, and the members of the EAB.
5. Redefining the algorithms and identity conceptual models (entities, attributes, relationships) if required.
6. Setting up the SPIRIT Regulatory Model (SRM) to monitor all milestones and stages of development.
7. Defining the ethical rules following the legal requirements coming from the European, national and regional legislation and guidelines of Art 29 Working Party.
8. Setting a privacy ontology model seeking for (i) interoperability, (ii) embedding privacy protections into the system, reusing some parts of the ongoing general GDPR ontology.
9. Integrating (i) anonymization, (ii) encryption, (iii) privacy preserving algorithm developments, (iv) and authorisations, into SRM.
10. Reassuring that all LEAs that participate in the project will receive the SPIRIT guidelines to use the platform according to the SPIRIT Regulatory Model. Including in the dissemination plan strategies to communicate the project to, whenever possible, a general audience, in order to create an opportunity for dialogue on potential concerns about the balance between, on the one hand, the need to develop new technologies for fighting crime and terrorism and, on the other hand, the protection of citizens' fundamental rights.

Figure 15 illustrates this indirect strategy to implement DPbD. General Data Protection Principles have been turned into specific modelling actions: (i) enforce, (ii) demonstrate, (iii) control, (iv) inform, (v) minimise, (vi) abstract, (vii) separate, (viii) and hide. External and internal controls have been set for: (i) Data access, (ii) Data collection, (iii) Data reuse and transfer, (iv) Data protection controls.

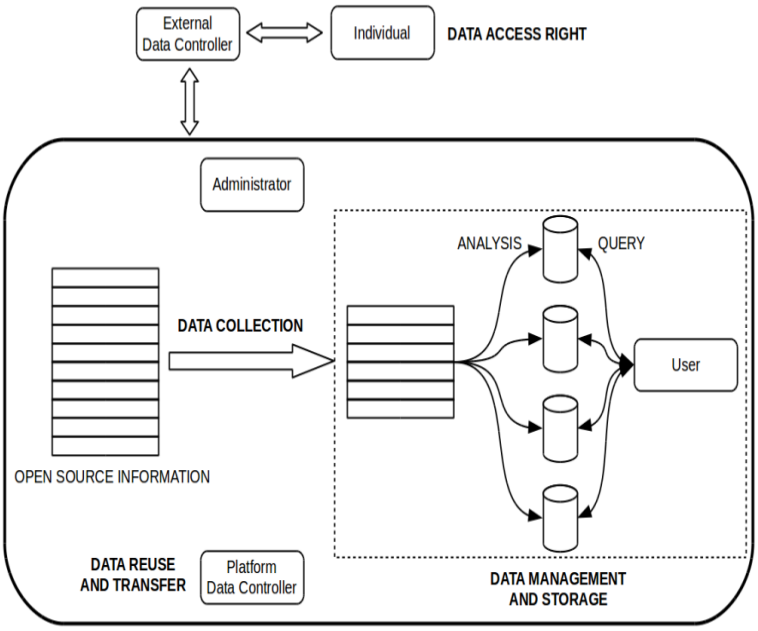


Fig. 15. SPIRIT Indirect strategy embedding data protection controls.

4.5. Incidental Risks Mitigation Policy (Residual risks): Towards an operational method of preventing abuse of the SPIRIT system by individuals and organisation

SPIRIT will provide an invaluable tool for law enforcement agencies and others to identify potential terrorist, drug-related, money laundering, and other breaches of laws. It will do this by collating and presenting large databases of social media, video and email etc. data which originate with individuals. Even if the individual is already identified as a criminal (in the relevant domain) their rights to privacy etc. need to be respected.

SPIRIT seeks to identify methods whereby privacy of individuals whose social media etc. posts are being viewed, through operational, legal, IT or procedural constraints on the users of the system.

Anonymisation of the data reduces the value of the data to investigators, and de-anonymisation seems to be possible in many cases, which limits the value of this as a privacy-protection mechanism. Different degrees of pseudonymisation are possible, and different methods will have different effects both on usability and on the ease with which de-anonymisation can be achieved.

In the broad sense, we seek to find methods whereby those who use the SPIRIT system comply with relevant legal, regulatory, social and ethical requirements in doing so. This includes only using the system for the specific purposes for which it is authorised, and not using it for other purposes.

A variety of risks have been identified in previous work, including risks related to:

- The lawfulness of processing
- Specification of purpose
- Breaches of the data minimisation principle
- Inaccuracy of data
- Data storage and retention
- Data security
- Access rights
- Information rights
- Accountability and Monitoring

Risk mitigation procedures are being developed to counter these risks, some of which involve technological or physical measures. But many of the risks relate to non-authorised or/and even inappropriate use of the data by individuals within the law enforcement agencies, or by the leadership of those agencies. These are harder to mitigate through rules, penalties etc. So, it is necessary to develop a methodology whereby the system is only used by those deemed to be trustworthy.

In addition to a regular incidental finding policy, we therefore suggest that a licensing system be developed for the use of the system, which could include the following features.

- Individuals within the law enforcement agencies who are to use the system should be carefully screened for past convictions, misdemeanours or unethical behaviour.
- Psychological screening should be carried out prior to any individual being given a licence.
- Taken together, these should be used to create a ‘suitability score’ for each individual who will be given access to the system.
- Use of the system by each individual should be monitored carefully, with usage that is deemed illegal, in breach of regulations or unethical generating a reduction in the suitability score.
- If the score falls below a pre-determined level, appropriate to the task being undertaken, then the licence to use the system will be withdrawn.

Project funded by H2020 Programme – Grant Agreement number: 786993

- Major breaches of security – for example allowing another individual to access the system on their behalf, or being careless with access etc. – will involve immediate suspension of the licence.
- Law enforcement organisations and departments within those organisations will also be scored. These scores will be a weighted aggregate of the scores for those individuals who are granted access, plus some scoring of the organisations past record on relevant matters.
- If the organisation is found to have behaved in a way which is deemed in breach of regulations or unethical this will generate a reduction in the suitability score for that organisation.
- If organisations score falls below a pre-determined level, access to the system will be withdrawn, pending an investigation. It will only be granted again if relevant safeguards, retraining etc. have been introduced.

We can also identify the requirements for each type of law enforcement activity for which the system might be used. Some will require less intensive/intrusive investigation than others. So it may be helpful to develop the SPIRIT system to provide different levels of information, for example with more or less anonymization.

If this is done, the suitability scores required to be granted access to each level of the system could be set at different levels, so that those with lower legal, regulatory, social or ethical standards could be granted more limited access. Table 3 summarises these policies to reduce incidental risks.

Table 3. Source of incidental risks and mitigation policies

Categories	Data sources to identify possible prevalence	Policies to reduce risks and their impact
Individuals		
Use for personal career advancement	Salary and bonus data	Licensing
Corruption + selling access to data	Press reporting of past events	Training
Vendettas against groups or individuals	Complaints against LEAs	Ongoing monitoring of usage

Deals with contacts in criminal-commercial organisations		Scoring of users
Mistakes, incompetence, inattention	Previous inquiries into LEAs	Alarm systems embedded in software
Embedded practices, legacy systems		Ontologies
LEAs		
Inadequate management	Inquiries into LEAs	Registration of LEAs
Weak governance	Annual reports	Responsible, dedicated officers
Lack of accountability	Reporting processes	Accountability and reporting
Relationships with other agencies	Internal government reports	Ongoing monitoring
Inter-departmental rivalries		Scoring of LEAs usage
Political		
Electoral gerrymandering	Press coverage of previous behaviour	Independence of process
Vendettas against groups – e.g Jews, migrants…	Complaints	Ethical Committee monitoring
Discriminatory policies, bias		Powers for EC to censure countries
Damaging political opponents	Survey data	
Finding scapegoats	Case studies	
External		
Professional hackers	Vulnerability assessments	Tracking processes
Foreign governments - eg China, Russia	Risk assessment by security services	Access procedures

European Commission | Horizon 2020 European Union funding for Research & Innovation

Project funded by H2020 Programme – Grant Agreement number: 786993

Blackmail of officials		Preventing breaches, restoring system
Dark Web	Reports of DW activity	Data protection officers
Virus-ransomware	Techical assessment of current threats	Anti-virus and ransomware
Bankruptcy-failure of operating company	Due diligence on company	Shut-down criteria
Reputational		
Highlighting of system failures	Past press reports on government systems	Complaints processes
Lobbyists	Surveys of public officials	Ombudsman-arbitration
Technological failures	Technical assessment of robustness	Compensation, Mediation

4.6. Incidental Risks Mitigation Policy (Residual risks): SPIRIT Regulatory Model

There is another dimension of risks that should be treated from a systemic approach. Directive 2016/680 (EU) explicitly mentions pseudoanonymisation as a method for handling data minimisation:

> Member States shall provide for the controller, taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing, as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, both at the time of the determination of the means for processing and at the time of the processing itself, *to implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing, in order to meet the requirements of this Directive and protect the rights of data subjects*. (Art. 20.1)
>
> Member States shall provide for the controller to implement appropriate technical and organisational measures ensuring that, *by default, only personal data which are necessary for each specific purpose of the processing are processed*. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that *by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.* (Art. 20.2)

A detailed method has been described in the *SPIRIT Reply to the Ethics Second Assessment Report, April 30st 2018, section 4. and ff*. : (i) to avoid that data may be "likely to be re-identified" a clear

separation has been made between identified data and de-identified or anonymised data, (ii) the Valcri anonymised data set has been developed in compliance with the applicable standards, (iii) confidentiality agreement will be signed prior to the use of the Valcri data set by all partners and all researchers involved in the SPIRIT project; (iv) a policy has been designed to deal with the potential residual risks of re-identification.

To monitor these processes a SPIRIT Regulatory Model will be set, plotting, mapping and following all information processes that will take place on the platform (Fig. 16), in connection with Fig. 15. This model will include all regulatory sources (hard law, soft law, policies and ethics) endorsed as smart (or better) regulations by the EU strategy to embed protections into computational systems. Data collected and processed will not be held or further used unless this is essential for reasons that are clearly stated in advance to support data protection. Such a model will integrate computational measures (e.g. ontologies) with data management and organisation.

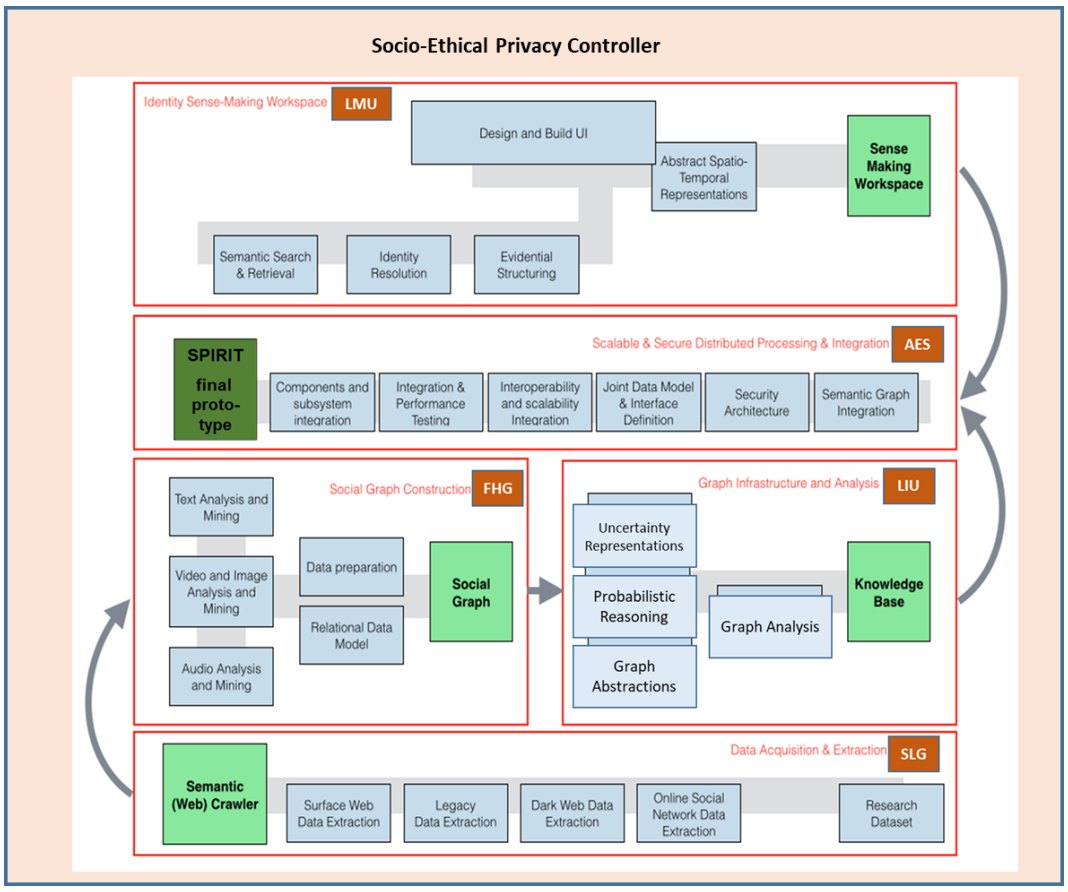


Fig. 16. SPIRIT System Architecture: Main Architectural Components

SPIRIT DoW includes the following capabilities and technical elements to be developed:

1. Data Acquisition and Extraction: Semantic capabilities, Dark web capabilities, Online social network capabilities, multi-purpose semantic crawler.
2. Social Graph Construction: Text analytics and mining, speech and audio analytics and mining, video and image analytics and mining, social graph modelling.
3. Graph Infrastructure and Analysis: knowledge management and graph analysis, data processing systems.
4. Scalable & Secure Distributed Processing & Integration: security and data protection measures, security evaluation, security semantics.
5. Identity Sense-Making Workspace: search and retrieval, data exploration, semantically supported data manipulation interactivity, automated data mining tools, cognitive support, collaboration.

Thus, minimisation will be implemented and evaluated within a middle-out strategy (i) stemming from the control of information flows, (ii) and eventually testing LEAs' and researchers' behaviour.

5 End-Users' Contribution (LEAs' Consultation)

5.1 LEAs' Preliminary Responses

To start working on the SPIRIT mitigation strategy, we asked for LEA's cooperation. We have prepared one preliminary consultation about LEAs' incidental findings policies (basically to know whether they had it or not). We defined incidental findings as any information gathered during an ongoing investigation which is not related to the purpose of the investigation, but that may affect or jeopardize the individual rights of citizens who are innocent or might not be involved in the investigation. Table 4 details the actions, time and reception of LEA's responses. We reproduce the consultation and LEA's answers in Annexes 3 and 4.

Table 4. Actions taken

Date	Event
28/9/18	IDT sent the Incidental Findings consultation to the police forces involved in the project. Deadline to receive the replies: 3/10/18
1/10/18	WSPOL (Poland) sent its reply
2/10/18	SERBLEA (Serbia) sent its reply
2/10/18	Thames Valley Police (UK) sent its reply
4/10/18	The IDT-UAB sent to the police forces a gentle reminder
8/10/18	West Midlands Police (UK) sent its reply
10/10/18	WSPOL (Poland) sent a clarification email related to its previous answer

10/10/18	Antwerpen Police (Belgium) sent its reply
22/10/18	Hellenic Police (Greece) sent its reply

It is worth noting that this is the starting point of a collaboration that is deemed to be continuous all along the development of SPIRIT. This will facilitate the updating of DPIA at every stage of the project.

Feedback has been quite concise and diverse so far. Antwerpen Police (Belgium) replied that they don't have any policy for incidental findings. Thames Valley Police (UK), and West Midlands Police (UK) referred to laws and internal policies, although without describing them or specifying police practices. WSPOL (Poland) and SERBLEA (Serbia) has sent useful information (and WSPOL a clarifying note):

> **[SERBLEA: Handwriting]** Law on personal data protection tell us that the processing of personal data is not allowed if the data being processed is unnecessary or inappropriate for the purpose of processing.
>
> This law does not tell us what to do with such data, so we remove them (delete them) for practical reasons (due to the space on the memory devices). The Commissioner for the Protection of personal information may order the deletion of data, but only if they are unlawfully collected, not if they have no relation to the purpose of investigation.
>
> All data my service collects are classified by the degree of secrecy -strictly confidential- the law that protects such data is much more restrictive.
>
> **Clarification [WSPOL: typewriting, fragment]**: The general rule is that if we obtain information about the crime or criminals that indicate a direct threat to human life and health, appropriate and adequate actions will be taken.
>
> If the information relates simply to another offense, it may be the basis for initiating a separate investigation. The condition is to carry it out completely and establish other evidences confirming crime conduct and the guilt of a specific person. When it comes to interviewing people and making statements in the investigation, we have, of course, specific regulations, rights for a witness or a suspect, about which we are obliged to warn persons before starting an activity. These regulations indicate that the witness may refuse to answer the question if the answer would involve criminal liability for him or for the closest person. The suspect has the general right to refuse to provide explanations or answers to specific questions. These are obvious procedural guarantees that are to secure the rights of individuals to avoid self-incrimination.

Hellenic Police (Greece) sent an answer expressing what we think can be a general statement: we have them, this is an internal matter, we cannot disclose them:

> *Question*: If the Incidental Findings policy is described in a document, is this document publicly available?
> *Answer*: No.
> *Question*: If these internal protocols, guidelines or best practices related to incidental findings are not described in a document, could you provide some information regarding your procedures when an incidental finding occurs? What do you do in these situations?
> *Answer*: If during an ongoing investigation an incidental finding is occurred, this finding is most likely that will fall within a certain area of competence, for which internal protocols, guidelines or best practices would exist.

We are proceeding under a general assumption of trust. Criminological investigations have shown that regulations play a role and have an impact on police behaviour. Hence, privacy and data protection should be added to the "law of the police" (Harmon, 2012) — the body of federal, state, local, and international law that applies to police officers and departments and influences what they do, according to Stoughton (2014).[14]

As we will specify later (Section 5.3), a common workshop with end-users to elicit such an information, all guarantees set, will help us to refine the recommendations and update the DPIA. This initiative and the educational training are elements of the SPIRIT systemic approach.

5.2 Impact of GDPR and DPJ on Policing

To our knowledge, there are no empirical studies about the impact of GDPR regulation on the behaviour of European Polices yet.[15] But there certainly are many academic coincident works showing that GDPR regulatory body has been designed to reframe police practices as well, implementing the other side of GDPR, namely the provisions contained in EU Directive (EU) 2016/680.

Since the Area of Freedom, Security and Justice was included in the new Treaty of Lisbon signed on 13 December 2007, ethics, law and best practices have been increasingly considered to set LEA's practical regulatory body, along with Europol, Eurojust and the European Union Prosecutor's Office (Ladenburger, 2008). This entailed a harmonisation effort, followed up by GDPR and the new regulations on policing. The Directive has been well-received (De Hert and Papakonstantinou, 2016). Marquenie (2017) also stresses its benefits but points out that "the Directive is unlikely to mend the

[14] See also Wilson (1976), Harmon (2012).
[15] In his work on police technology usage, Custer (2012) found that Wiretapping and GPS/position tracking devices were used by 100% of the LEAs particpating in the study, while only 26% used Privacy Enhanced Technologies (PET). The percentage increased to 33 % in his second survey (Custer and Vergouw, 2015).

fragmented legal framework and achieve the intended high level of data protection standards consistent across European Union member states" (ibid.: 324).[16] Policing and law-enforcement is deemed to be a national issue, linked to national-states sovereignty.

Jasserand (2017) highlights that safeguards could have been even stronger, compared to case law.[17] She reminds the "huge amount of law enforcement requests made to high-tech companies at global level, the case of the transfer of passenger name record data (air traveller data) to police authorities, and the retention of telecommunications data by Internet Service Providers (personal data retention) for further use by law enforcement authorities" (ibid. 2017: 154-155).

Cross-border coordination among Data Protections authorities to respond to data breaches incidents constitutes another problem yet to be solved. The outcomes of the 1st Pan-European Personal Data Breaches Exercise were illuminating. It was conducted at the end of 2015 by the Directorate-General Joint Research Centre in collaboration with the Directorate-General for Justice and Consumers of the European Commission and the Data Protection Authorities of seven EU Member States. Among other results, the authors addressed the lack of: (i) a single point of contact list, (ii) technical means for the agile and reliable exchange of information, (iii) harmonized procedures to support cooperation in the handling of cross-border incidents of personal data breaches. Language uses, difficulties in the harmonised interpretation of applicable law, and the need to harmonise and facilitate the secure exchange of information were also pointed out (Malatras et al, 2016: 467-68).

Purtova (2018: 52) highlights that "one of the problems with GDPR is which legal regime applies when private entities and law enforcement act as joint controllers is a grey area of the dual EU data protection regime and may seriously undermine legitimacy of Public-Private Partnerships". The Budapest Convention Cybercrime (2001)[18] does not address this problem either, although its Preamble reads that it recognises "the need for co-operation between States and private industry in combating cybercrime and the need to protect legitimate interests in the use and development of information technologies". The dual alleged situation we experience at present is far from its

[16] "[…] while making vast improvements to the substantive level of data protection, the Directive leaves parts of the current fragmented framework unaltered. Article 60 explicitly states that specific provisions covering data protection in already existing Union legal acts shall remain unaffected, and while article 61 originally set a fixed time table for the amendment of previously concluded international agreements in this field, the final version of the text stipulates that they shall remain in force until otherwise amended, replaced or revoked." (Marquenie, 2017: 329).

[17] Jasserand tested the provisions contained in Directive 2016/680 against the standards established by the ECJ in Digital Rights Ireland and Tele2 Sverige on the retention of data and their further access and use by police authorities. Her analysis reveals that Directive 2016/680 does not contain the safeguards identified in the case law.

[18] Council of Europe's Convention on Cybercrime (ETS No 185). 23/11/2001. http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf

primarily objectives of harmonising substantive law on cyber-crime across borders, and procedural laws applicable to criminal investigations with a digital component (Tosoni, 2018).

5.3 UAB Survey (questionnaire) to elicit LEAs' information

Having this situation before us, we will take a proactive stance within the SPIRIT project. We should also carry out a balanced approach between police needs and the proliferation of constraints that could represent a burden or hinder LEAs' everyday work. We do not advocate that more regulations or more complex norms are helpful. As already stated in the literature, "stronger legal protection may lead to weaker consent in data protection" (Schermer et al. 2016). Our own experience in dynamic DPIAs is that cooperation is always a better option than unwanted interventions that could be interpreted as intrusive (Casanovas et al. 2014).

Hence, we designed a questionnaire (Annex 5) —i.e. a survey, not a consultation, to be sent after the signature of an informed consent form— to seek information from LEAs which will enable us to calibrate the risk model. As we detail in the Annex, we'll hold a specific Workshop with LEAs to elicit this kind of internal information through focus groups techniques.

We need to know what the likelihood of incidental actions is leading to breaches of privacy and other untoward effects. These actions could originate from individuals within LEAs, from the LEAs themselves, from politicians and from external actors, including those who seek to bring the system into disrepute. Once the model is suitably calibrated, in part using the responses to this second questionnaire, we will then be able to refine the mitigating policies, which in turn will enable us to reduce the residual risk to a minimum. This questionnaire has been discussed and approved by the EAB. Report on the discussion can be found in the EAB First and Second Screening Reports, annexed to Deliverable 9.5.

5.4. Results from the UAB Survey

The questionnaire was distributed to all the LEAs end-users in SPIRIT. We collected 4 replies that can be found in Annex 8. The results of the questionnaire where used to design the second consultation (Section 5.5.) and to update the policies (Section 5.6)

5.5. Second consultation: LEAs Workshop: Refining SPIRIT Incidental findings and risks policies

Objectives of the Workshop

The SPIRIT project held the LEAs WORKSHOP: Refining SPIRIT Incidental findings and risks policies, on the 10th of June, at Wolfson College in Oxford. The workshop was organised by the ethical lead partner, the IDT-UAB, and lead by one of the external advisors on the SPIRIT Incidental Findings, Prof. Nicholas Morris (PhD). The aim of the workshop was to complete the incidental risk assessment- as included in D.9.2- for developing a comprehensive policy to address the incidental risks of SPIRIT. Prof. NicholasMorris (PhD), Sue Jaffer and

Prof. John Howell (PhD) participated in the Workshop as external advisors. Their participation was accepted by the SPIRIT Consortium and they all signed confidentiality agreements that can be found in Annex 6.

The workshop gave SPIRIT researchers and external advisors the chance to better understand the potential issues of breaches of privacy, inappropriate or wrongful release of personal data and identity data, in police work, among other significant and challenging issues that need to be carefully addressed from a legal and ethical perspective. This was possible due to the great support and collaboration of the SPIRIT LEAs. Trough participatory methods that included several practical exercises, LEAs reflected and shared their expertise on incidental risks, risk minimising strategies and structures in place in their organisations and room for improvement on how legal and ethical values, principles and requirements should be addressed by LEAs in their day-to-day processing of personal data.

Additional documentation on the Workshop such as the agenda, the attendance list can be found in Annex 7, and Nicholas Morris presentations can be found in Annex 8.

Methodology

In order to elicit expert knowledge from the LEA representatives to modulate and update the incidental findings and incidentals risks policy the UAB-IDT designed and conducted two participatory exercises.

The first exercise consisted on seven cases that were presented to the LEAs to generate an open discussion. The cases, reproduced below, were designed to address each of the source risks and categories included in the Incidental Risk Matrix as presented in D9.2. For each of the cases the researchers presented three questions:

1. How will your organisation detect/uncover this situation?
2. Describe the procedure to address this situation.
3. Recommend other ways to improve how your organisation manages these issues.

INDIVIDUALS

CASE 1: A police officer is currently up for promotion together with other four colleagues from the organisation. In order to be better prepared and obtain the promotion the officer uses technological tools to which he has access for crime investigation purposes, to access data, including email and social network profiles, from competitors and from the members of the evaluation board.

CASE 2: A Police officer with ties to a radical right group sells to this group personal data of migrants that are residents in the area. This includes data such as name, address, work address, phone number and email and content from their social network accounts (places where they checked, photos, etc).

LEAS

CASE 3: A medium rank officer transfers personal data from a suspect to a colleague from a different agency. This is something that he usually does since there is a data sharing agreement. However, this particular transfer is done after the agreement has been suspended due to suspicions that the other agency is misusing such data. The officer sending the data was not aware of this situation, he did not receive any notification on the matter and he did not check the validity of the agreement, he acted according to the embedded practices of his organisation.

POLITICAL

CASE 4: An officer receives from one of the candidates for being local Mayor a request to provide him with damaging information, including personal data, on another one of the candidates that represents a racial minority community. The officer provides this information in exchange for the payment of a sum of money. Nut also because he defends racist ideas.

EXTERNAL

CASE 5: A group of professional hackers attacks your system. They access all the personal information from the officers (including name, address, phone, email and personal records on disciplinary procedures). They request a sum of money as ransom for the data.

CASE 6: Your organisation is conducting a cover investigation in the Dark Web. Your organisation creates a trap on the Dark Web to "attract" dealers in weapons. One of the dealers blackmails one officer participating in the operation into giving him personal data from competitor criminals. If the officer does not accept, the operation is compromised because they know he is a police officer.

REPUTATIONAL ATTACKS

CASE 7: A very relevant local TV station receives information from a whistle-blower. He claims to be a police officer that has information on a generalised data breach of the police database that affects thousands of citizens. The TV stations start an intense campaign to uncover what happened. The breach actually happened due to a technological failure in the police network and computer systems.

In the second exercise, LEA representatives were provided with a list of all the categories of risk identified in the Incidental Findings Matrix in D9.2 and asked them to rate according to their perception, the likelihood that any of those events may occur. The rating scale available to reply were L=Low, M=Medium, H= High. The replies of the LEAs to the second exercise carried out during the workshop are included in Annex 9 after anonymization of the respondents' organisations for confidentiality reasons. The replies included the name of the LEA of the respondents, and some respondents decided to voluntary write their name. However, and giving that this deliverable is Public, both the name of the organisation and the respondents have been anonymized. Table 7 shows the aggregated results for each of the events.

EVENTS	RATE (Total replies)
Misuse of data for personal career advancement	6L
Corruption and selling access to data	6L
Individual vendettas against groups or individuals	6L
Deals with contacts in criminal-commercial organisations	6L
Mistakes, incompetence, inattention	6M
Breach of privacy and data protection in embedded practices, legacy systems	3L; 2H; 1M
Inadequate management	3L; 3M
Weak governance	5L; 1M
Lack of accountability	5L;1H
Breach of privacy and data protection in relationships with other agencies	3M; 3L
Inter-departmental rivalries	6L
Electoral gerrymandering	5L;1M
Political vendettas against groups	5L; 1 No Answer
Discriminatory policies, bias	6L
Finding scapegoats	6L
Hacking of your systems by professional hackers	3L;3M
Hacking of your systems by foreign governments	4M; 1L-M;1L
Blackmail of officials	5L;1M
Breach of privacy and data protection on the Dark Web	2L;1H;1M;1M-H
Virus/ransomware	4M;1L;1L-M
Bankruptcy-failure of operating company	6L
Highlighting of your system failure (by the press, Human rights advocates, NGOs)	4L;2M
Issues derived from Lobbyists	6L
Technological failures in your systems	6M

Table 7: Aggregated results to the second exercise

5.6. Results of the LEAs Consultations: Update of the policies

The responses gathered in the Workshop were then used to update the incidental and residual risks model previously described in Deliverable N° 9.2: Incidental Findings Policy (WP9).

The responses outlined above were used to update the likelihood rankings for each category of incidental risk, as follows:

- Based on majority vote by seminar participants
- In the case of a tie (equal numbers for each level) upper level taken
- Bold, black numbers in what follows mean original score accepted by participants
- Red numbers mean score changed (usually downgraded – ie lower probability of a problem)

Almost always, the participants gave lower risk scores than were hypothesised initially. The only exception is 'Technological failures in your systems", where they think it is more likely than initially assumed (upgraded from L to M). Overall, the weighted average risk falls from 22.9% to 13.7%. After the mitigation strategies outlined in Deliverable 9.2, the residual risk falls from 5.0% to 3.3%.

The Matrices which follow are presented the same format as in Deliverable 9.2, for ease of comparison.

Wrapping up the outcomes of the Oxford Workshop,(i) LEA's responses were used to update the likelihood rankings for each category of incidental risk, (ii) the IDT team drafted a summary (a handbook) of legal and ethical SPIRIT policies as a set of practical guidelines to be followed

by all members of the consortium, (iii) one important finding was that EU Polices agreed on maintaining the rules about incidental findings (for researchers) and incidental risks (for LEAs). Rules (See Section 2.2.1, above) could be kept at the core of legal and ethical SPIRIT set of principles according to their substantive and procedural dimensions. As already stated, after the mitigation strategies outlined in Deliverable 9.2 and the refining of scores and matrices, the estimated residual risk has fallen from 5.0% to 3.3%.

However, there are still some issues left, as it is not possible to eliminate all residual risks. LEAs commented in the workshop on the deep cultural and technological changes experienced by the population and how they are affecting the attitudes towards vulnerable minorities. The production of false positives could be linked not only to misfunctions of the technical system but also to previous implicit attitudes assumed both by researchers and by police investigators. Best practices and professional culture matter, and there are extended references in the literature as well to both aspects, the positive side of fair police culture, and the presence of cognitive, distributional and cultural biases.[19] Moreover, the possibility of corruption cannot be completely eliminated from any organisation. Thus, regular checking and multilayered audits are important

[19] The notion of distributional bias is related to the use of technology in providing public services. E.g. Clark, B.Y., Brudney, J.L. and Jang, S.G., 2013. "Coproduction of government services and the new information technology: Investigating the distributional biases". *Public Administration Review*, 73(5), pp.687-701.

to recalibrate a balanced and fair use of investigative technologies. Avoiding "overpolicing" entails fostering both trust and security through internal and external controls that should be put in place to protect citizens' rights.[20]

[20] Susan Jaffer handwritten *Notes* at the Oxford Seminar.

Incidental Risk Analysis	Revised Scoring based on Oxford seminar responses				
		A	B	C	A*B*C
Source of Risk	Categories	Source likelihood (%)	Likely incidence of risk category (H, M, L)	Weight (as % source)	Risk Incidence
Individuals	Use for personal career advancement	30	L	20	0.6%
	Corruption + selling access to data		L	10	0.3%
	Vendettas against groups or individuals		L	10	0.3%
	Deals with contacts in criminal-commercial organisations		L	5	0.2%
	Mistakes, incompetence, inattention		M	30	1.8%
	Embedded practices, legacy systems		**M**	25	1.5%
	personal gain eg family, girls etc.			**Total**	**4.7%**
LEAs	Inadequate management	10	M	30	0.6%
	Weak governance		L	20	0.2%
	Lack of accountability		L	30	0.3%
	Relationships with other agencies		**M**	10	0.2%
	Inter-departmental rivalries		L	10	0.1%
				Total	**1.4%**
Political	Electoral gerrymandering	20	L	25	0.3%
	Vendettas against groups - eg Jews, migrants		L	20	0.2%
	Discriminatory policies, bias		L	20	0.2%
	Damaging political opponents		L	20	0.2%
	Finding scapegoats		L	15	0.2%
				Total	**1.0%**
External	Professional hackers	30	M	40	2.4%
	Foreign governments - eg China, Russia		M	20	1.2%
	Blackmail of officials		L	10	0.3%
	Dark Web		**M**	10	0.6%
	Virus-ransomware		M	10	0.6%
	Bankruptcy-failure of operating company		L	10	0.3%
				Total	**5.4%**
Reputational attacks	Highlighting of system failures	10	L	50	0.5%
(by press etc?)	Lobbyists		**L**	30	0.3%
	Technological failures		M	20	0.4%
Total		**100**		**Total**	**1.2%**
				Overall	**13.7%**
			H	30%	
			M	20%	
			L	10%	
			As % opportunity		

European Commission | Horizon 2020 European Union funding for Research & Innovation

Project funded by H2020 Programme – Grant Agreement number: 786993

Revised Scoring based on Oxford seminar responses					
Development of Mitigation Policies					
Data sources to identify possible prevalence	**Policies to reduce risks and their impact**	**Mitigation effect (% reduction in overall source risk)**	**Residual risk**		
Salary and bonus data	Licensing	5			
Press reporting of past events	Training	10			
Complaints against LEAs	Ongoing monitoring of usage	20			
	Scoring of users	10			
Previous inquiries into LEAs	Alarm systems embedded in software	10			
	Ontologies	10			
	Total for source	**65**	**1.6%**	**Total for source**	
Inquiries into LEAs	Registration of LEAs	10			
Annual reports	Responsible, dedicated officers	30			
Reporting processes	Accountability and reporting	10			
Internal government reports	Ongoing monitoring	10			
	Scoring of LEAs usage	10			
	Total for source	**70**	**0.4%**	**Total for source**	
Press coverage of previous behaviour	Independence of process	20			
Complaints	Ethical Committee monitoring	40			
	Powers for EC to censure countries	20			
Survey data					
Case studies					
	Total for source	**80**	**0.2%**	**Total for source**	
Vulnerability assessments	Tracking processes	20			
Risk assessment by security services	Access procedures	20			
	Preventing breaches, restoring system	10			
Reports of DW activity	Data protection officers	10			
Techical assessment of current threats	Anti-virus and ransomware	10			
Due diligence on company	Shut-down criteria	10			
	Total for source	**80**	**1.1%**	**Total for source**	
Past press reports on government systems	Complaints processes	30			
Surveys of public officials	Ombudsman-arbitration	20			
Technical assessment of robustness	Compensation	10			
	Mediation	10			
	Total for source	**70**	**0.0%**	**Total for source**	
			3.3%		
	Note: mitigation cannot bring matters to below zero				

European Commission | Horizon 2020 European Union funding for Research & Innovation

Project funded by H2020 Programme – Grant Agreement number: 786993

6 Recommendations: Summary

6.1 Incidental Findings in the Research Context

Some of the Recommendations from *ANTICIPATE and COMMUNICATE. Ethical Management of Incidental and Secondary Findings in the Clinical, Research, and Direct-to-Consumer Contexts* (2013) could be also useful to the security domain. Especially (i) Informing Persons Tested, (ii) Evidence-Based Practice Guidelines, (iii) Additional Empirical Research, (iv) Education and training provided to stakeholders, (v) Principles of Justice and Fairness, (vi) Context-specific recommendations. Others are specifically designed to prevent unbalanced situations of power in the security area.[21] Table 5 reproduces the Ethical Principles in the Research Context (2016). These principles should be applied (i) jointly with the Fair Information Practices and DPbD Principles that are much more known in Computer Science, (ii) along with all data protection principles contained in the GDPR and DPJ provisions: fair processing, minimisation, anonymisation etc. (see Art. 4 Directive EU 2016/680).

Table 5. Ethical Principles in the Research Context, adapted from the US Presidential Commission for the Study of Bioethical Issues (2016)

Principle	Definition	Application
Respect for persons	This principle recognizes the fundamental human capacity for rational self-determination.	Researchers must communicate the fundamental aspects of their research – including the possibility of discovering incidental or secondary findings and the plan for their disclosure or management – so that participants can make informed decisions about whether to enroll.
Beneficence	This principle calls on professionals to take action to ensure the wellbeing of others. Its corollary, non-	This principle supports returning findings when disclosure might help forestall or prevent harm. By contrast, disclosing an incidental finding for which no preventive or positive action can be taken has

[21] According to the Presidential Commission for the Study of Bioethical Issues (2016), Incidental findings can be either "anticipatable" or "unanticipatable." An anticipatable incidental finding is one that is known to be associated with a test or procedure. Anticipatable incidental findings need not be common or even likely to occur—their defining characteristic is that the possibility of finding them is known. Unanticipatable incidental findings include findings that could not have been anticipated given the current state of scientific knowledge. Researchers cannot plan for these types of findings specifically. However, they can consider in advance what they might do if a particular kind of unexpected finding arises, for example, one that could be actionable or lifesaving.

	maleficence, requires not imposing harm on others.	the potential to cause anxiety and distress with no corresponding benefit.
Justice and Fairness	This principle requires fair and equitable distribution of the potential benefits and burdens across society.	The principle of justice and fairness calls upon researchers to take into account how policies for returning incidental and secondary findings could benefit or burden some participants or, alternatively, could burden the research enterprise and the ability to contribute to generalizable knowledge.
Intellectual Freedom and Responsibility	This principle protects sustained and dedicated creative intellectual exploration that furthers scientific progress, while requiring that researchers take responsibility for their actions.	This principle supports affording wide latitude to researchers in pursuing their scientific goals and engaging in intellectual exploration for the good of society, while also expecting that researchers uphold and respect the trust placed in them by participants. Ethical conduct of research with human participants includes acknowledgment and planning for incidental and secondary findings.

We would like to draw attention to the fact that, as said, the implementation of principles is not only an ethical issue, but an organisational one, i.e. a matter of good governance and smart regulation. Art. 4.f of the DPJ assesses that member states shall provide for personal data to be "processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, *using appropriate technical or organisational measures* [our emphasis]".

This means that along with data protection by design and by default, other measures related to organisational principles may also apply. From a computational approach *semantic interoperability* should be differentiated from *systemic interoperability* (Casanovas et al. 2017b). Accordingly, what our Recommendations should consider is not just semantic (or information processing) security, but *systemic security*: (i) the outcome of the convergence between security and safety measures, (ii) the implementation of an incidental and residual risks policy to reduce them as much as possible, (iii) *and* the structural and organisational approach that brings together human and computational means to create a fair and effective ecosystem. This is aligned with Recital 34 of DPJ 2016/680/EU , according to which

> The data subject should have the right not to be subject to a decision evaluating personal aspects relating to him or her which is based solely on automated processing and which produces adverse legal effects concerning, or significantly affects, him or her. In any case, such processing should be subject to suitable safeguards, including the provision of specific information to the data subject and the right to obtain human intervention, in particular to express his or her point of view, to obtain an explanation of the decision reached after such assessment or to challenge the decision. Profiling that results in discrimination against natural persons on the basis of personal data which are by their nature particularly sensitive in relation to fundamental rights and freedoms should be prohibited under the conditions laid down in Articles 21 and 52 of the Charter.

SPIRIT Recommendations on incidentals findings will follow this approach. They are deemed to be implemented in addition to the provisions contained in the original DPIA (Annex 1), and they carefully differentiate between (i) researchers (who cannot access to real cases being handled by LEAs), and (ii) LEAs' investigators and analysists (who are responsible for data processing under their national legal provisions, but also under GDPR and especially the transposable DPJ 2016/680)

6.2 The nature of potencial harm

The nature of potential harm matters to set SPIRIT Recommendations. I.e. Recital 61 of the EU Directive (EU) 2016/680 reads:

> A *personal data breach*[22] may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as *loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantag*e to the natural person concerned [our emphasis]. Therefore, as soon as the controller becomes aware that a personal data breach has occurred, the controller should notify the personal data breach to the supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless the controller is able to demonstrate, *in accordance with the accountability principle*, that the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where such notification cannot be achieved within 72 hours, the reasons for the delay should accompany the notification and information may be provided in phases without undue further delay.

Recital 62 reads:

[22] A "'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed", art. 3. 11 DIRECTIVE (EU) 2016/680.

> *Natural persons should be informed without undue delay* where the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, in order to allow them to take the necessary precautions. The communication should describe the nature of the personal data breach and include recommendations for the natural person concerned to mitigate potential adverse effects. Communication to data subjects should be made as soon as reasonably feasible, in close cooperation with the supervisory authority, and respecting guidance provided by it or other relevant authorities. For example, the need to mitigate an immediate risk of damage would call for a prompt communication to data subjects, whereas the need to implement appropriate measures against continuing or similar data breaches may justify more time for the communication. Where avoiding obstruction of official or legal inquiries, investigations or procedures, avoiding prejudice to the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties, protecting public security, protecting national security or protecting the rights and freedoms of others cannot be achieved by delaying or restricting the communication of a personal data breach to the natural person concerned, such communication could, in exceptional circumstances, be omitted.

Data breaches can led to identity theft, significant financial loss by the individual, threats to an individual's physical safety, loss of business or employment opportunities, humiliation, damage to reputation or relationships workplace, or social bullying or marginalisation. These situations should be anticipated and avoided both by researchers and LEAs, and proportionally balanced in a comprehensive case-by-case risk analysis. As stated by the recent Australian *Notifiable Data Breach* (NDB) contained in Part IIIC of the *Privacy Act* and applicable to breaches that occur on or after 22 February 2018:

> The NDB scheme provides entities with the opportunity to take positive steps to address a data breach in a timely manner, and *avoid the need to notify*. If an entity takes remedial action such that the data breach would not be likely to result in serious harm, then the breach is not an eligible data breach for that entity or for any other entity.[23]

Likewise, Art. 31 of DIRECTIVE (EU) 2016/680, specifies that "where the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, provide for the controller to communicate the personal data breach to the data subject without undue delay." But it also sets several exceptions. The communication to the data subject is not required if any of the following conditions are met: (i) the controller has implemented appropriate technological and organisational protection measures; (ii) the controller has taken subsequent measures which ensure that the high

[23] https://www.oaic.gov.au/agencies-and-organisations/guides/data-breach-preparation-and-response#part-4-notifiable-data-breach-ndb-scheme

risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise; (iii) it would involve a disproportionate effort.

SPIRIT Recommendations are following this path of both protecting and saving time, efforts and unnecessary trouble for the potential recipients. They are deemed to be implemented in addition to the provisions contained in the original DPIA (Annex 1), and they carefully differentiate between (i) researchers (who cannot access to real cases being handled by LEAs), and (ii) LEAs' investigators and analysists (who are responsible for data processing under their national legal provisions, but also under GDPR and especially the transposable DPJ 2016/680).

6.3. Recommendations on Incidental findings (Researchers)

[In addition to the DPIA]

1. Researchers should describe to potential recipients[24] incidental, secondary and discovery findings that are likely to arise or be sought from the tests and evaluations conducted. The principle of informed consent applies in all situations. Researchers should also clearly communicate to participants the plan for disclosing and managing anticipatable incidental findings.

2. In the case that a name corresponding to a real person had been de-anonymised, the researcher/developer that detects the problem must immediately notify AES, as the partner responsible for anonymisation in the SPIRIT project, and the SPIRIT DPO.

3. The SPIRIT DPO, after consulting with the EAB will decide and instruct AES on the following issues: (i) the need to notify and/or grant access to data to the person identified; (ii) the need to notify West Midlands Police, as owners of the data set; (iii) the need to erase the person's data from all data sets; (iv) the need to re-anonymise the person's data from all data sets.

4. Researchers should report to the SPIRIT Executive Board the incidental findings that could be a threat for citizens' rights. SPIRIT Executive Board will communicate and share it with the SPIRIT DPO, and the EAB members. They can decide alike about the steps to be taken upon discovery of incidental findings. According to the gravity of the incidence, they might consider whether to disclose or not to disclose the findings to the affected person. They can respect the person's preference not to know. However, exceptions should be discussed, argued, and documented.

[24] Art. 3, 10 ibid. "'Recipient' means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not".

5. The general principle of the right to know[25] and decide prevails *prima facie* in case of a personal data breach. The affected person should receive a report both about the incidence and the adopted solution. However, the level and nature of harm will be balanced prior to the communication according to Art. 13.3 of the DIRECTIVE (EU) 2016/680 (to protect public security, national security, and the rights and freedoms of others), and Art. 34 of EU Regulation (EU) 2016/679.

6. In response to the trust imparted to them, researchers owe society and research participants obligations to design and implement research in a responsible manner. No social discrimination should be tolerated. Any perception of a possible bias in the analysis or the performance of tests (due to technical failure or any other causes) should be reported.

7. Researchers should also develop a process for evaluating and managing unanticipatable findings. This is what this Deliverable (D9.2) is carrying out when turning incidental findings into incidental risks, and when reducing them as much as possible into remaining residual risks.

8. Companies, research units, universities, DPO and EAB members should be open to provide guidance and educational guidelines on ethical and legal privacy and data protection issues to all members of the Consortium (including especially the end-users of the system).

[25] This is grounded on Recital 46 of the DIRECTIVE (EU) 2016/680 in connection with Arts. 12 and ff. (rights of the data subjects). R. 46 reads: "A natural person should have the right of access to data which has been collected concerning him or her, and to exercise this right easily and at reasonable intervals, in order to be aware of and verify the lawfulness of the processing. *Every data subject should therefore have the right to know, and obtain communications about, the purposes for which the data are processed, the period during which the data are processed and the recipients of the data, including those in third countries*. Where such communications include information as to the origin of the personal data, the information should not reveal the identity of natural persons, in particular confidential sources. For that right to be complied with, it is sufficient that the data subject be in possession of a full summary of those data in an intelligible form, that is to say a form which allows that data subject to become aware of those data and to verify that they are accurate and processed in accordance with this Directive, so that it is possible for him or her to exercise the rights conferred on him or her by this Directive. Such a summary could be provided in the form of a copy of the personal data undergoing processing." See also Recital 63: "Every data subject should have the right to lodge a complaint with a single supervisory authority and to an effective judicial remedy in accordance with Article 47 of the Charter where the data subject considers that his or her rights under provisions adopted pursuant to this Directive are infringed or where the supervisory authority does not act on a complaint, partially or wholly rejects or dismisses a complaint or does not act where such action is necessary to protect the rights of the data subject". Also see Recital 63 of the REGULATION (EU) 2016/679: "A data subject should have the right of access to personal data which have been collected concerning him or her, and to exercise that right easily and at reasonable intervals, in order to be aware of, and verify, the lawfulness of the processing. This includes the right for data subjects to have access to data concerning their health, for example the data in their medical records containing information such as diagnoses, examination results, assessments by treating physicians and any treatment or interventions provided. *Every data subject should therefore have the right to know and obtain communication in particular with regard to the purposes for which the personal data are processed, where possible the period for which the personal data are processed, the recipients of the personal data, the logic involved in any automatic personal data processing and, at least when based on profiling, the consequences of such processing*".

9. Researchers should prepare educational materials to inform all investigators —including LEAs, occasional practitioners, and potential recipients— about the ethical, practical, and legal considerations raised by incidental, secondary, and discovery findings and risks.

10. Due to the sensitive nature of their work in SPIRIT, researchers will keep it confidential, especially for matters related to their relationships with LEAs. Scientific communications are nevertheless encouraged, under the supervision and previous approval of the SPIRIT Executive Board.

6.2. Recommendations on Incidental risks (LEAs)

[In addition to the DPIA]

1. The principles of justice and fairness require that all individuals (including LEA investigators) have access to adequate information, guidance, and support in making informed choices about how to proceed, what kind of information to seek, and what to do with the information once received. However, Directive 2016/680/EU allows LEA controllers to "assess, by way of a concrete and individual examination of each case, whether the right of access should be partially or completely restricted" (Recital 44).

2. LEAs must comply first with internal policies and standards at the regional and the national level, and with the legal provisions applicable to them. However, data protection and privacy has become a European matter, as the Regulation is directly applicable to all state members and the provisions of Directive 2016/680/EU have to be transposed into national law. Accordingly, while being the recipients of European research funds, LEAs should be compliant with the decisions made by the SPIRIT DPO and the Ethical Advisory Board related to ethics, incidental findings, and incidental risks management.

3. LEAs will attend the requirements of information on ethical and legal issues received from the SPIRIT Executive Board, the SPIRIT DPO and the SPIRIT EAB. In compliance with the recently enacted EU GDPR and Directive 2016/680/EU, agencies will cooperate closely with SPIRIT researchers to produce a dynamic and updated Data Protection Impact Assessment all along the project.

4. LEAs' agencies will evaluate regulatory oversight of the use of the SPIRIT platform to ensure safety and reliability. Regular internal controls will apply. However, due to the special sensitivity of personal information, an identifiable internal controller will be appointed, assuming the responsibility to act as DPO to facilitate the connection with the SPIRIT DPO all along the project.

5. LEAs will respect the foreseen policy for re-identified data, the Privacy preserving algorithm development, and the PbD ontology to comply with the SPIRIT regulatory model.

6. LEAs will provide true and reliable information to calibrate the risk model and minimise residual risks in accordance with the national and international applicable law that regulate LEAs' behaviour and practices.

7. A special license comprising all aspects of security (screening, scoring, monitoring) will be granted to operate within SPIRIT.[26]

8. Major breaches of security — for example allowing another individual to access the system on their behalf, or being careless with access, or breach of confidentiality or secrecy, or detection of discriminatory behaviour— will involve immediate suspension of the licence.

9. Law enforcement organisations and departments within those organisations will also be scored. These scores will be a weighted aggregate of the scores for those individuals who are granted access, plus some scoring of the organisations past record on relevant matters.

10. If the organisation is found to have behaved in a way which is deemed in breach of regulations or unethical this will generate a reduction in the suitability score for that organisation.

11. If organisations score falls below a pre-determined level, access to the system will be withdrawn, pending an investigation. It will only be granted again if relevant safeguards, retraining etc. have been introduced.

12. LEAs will set a redress procedure to amend possible damages in the case of false positives, leakages on the Web, or damages to personal reputation of individuals not involved in criminal behaviour. This will include a public announcement of apologies, mediation, arbitration and eventually compensation, depending on the severity of the incident and the legal system under which they operate.

[26] This recommendation is a preliminary step. It should be carefully balanced and discussed within the SPIRIT Consortium in the next months. A license is a legal instrument. As a matter of example, we include in Annex 7 a fairly simple license, Apache v2 - which underpins several opensource web crawlers such as Storm Crawler. It would need to be expanded to cover the data protection issues with the data —this is just for use of software to crawl public domain data. However, the Convention on Cybercrime (185) recognises "the need for co-operation between States and private industry in combating cybercrime and the need to protect legitimate interests in the use and development of information technologies". The aim of the Directive is also to facilitate the police work, and several Polices (end-users) are official partners. Exceptions apply. Recommendation n. 7 is due to the special nature of the SPIRIT project regarding crawling and identity. In the spirit of the GDPR and the Directive, the SPIRIT Consortium will discuss, evaluate, and come up with a proposal to be considered and discussed with the DPO and the EAB. As suggested by the Ethical Advisory Board these discussions will take place and will be included in the next Ethical and Legal Deliverables.

13. The redress system (point 12) will be subject to national legal provisions, case-based law, and LEAs' internal controls and guarantees. But especially in the SPIRIT testing phase, it will be also under the ethical and legal supervision and scrutiny of the DPO and the EAB. The EAB will have the ultimate power to prevent LEAs from using the system if the level of incidental risk is deemed to be below the acceptable threshold.

14. The nature of harm will serve as criteria for the EAB and DPO to decide about what kind of disclosure, notification and regulatory regime to apply in case of data breach, false positives, and any discovered or reported threat to personal data identity.

15. As stated by the Directive (art. 56), "any person who has suffered material or non-material damage as a result of an unlawful processing operation or of any act infringing national provisions" has the right to receive compensation for the damage suffered from the controller or any other authority competent under Member State law. This explicitly includes LEAs. The EAB and DPO, after ethical and legal advice, will decide which is the appropriate way to proceed to reach a reasonable degree of redress. This will happen even in the case that the Directive has not yet been integrated into the national legal system.

7. ANNEXES

ANNEX 1: SPIRIT PRELIMINARY DPIA

Data Protection Principle/Requirement	Legal Basis	Potential Risk	Mitigation measures	Preliminary Evaluation
Lawfulness Is the processing lawful?	Art 8 Directive (EU) 2016/680 Art 5.1 (a) Regulation (EU) 2016/679	Members of the Consortium other than those authorised by law, accessing and processing personal data	- Levels of access and conditions have been agreed with LEAs and are included in the signed Service Contract. - Personal data of citizens will only be processed in the evaluation phase by members of LEAs that are controllers of such data. - Personal data of citizens will only be processed by LEAs according to the legal framework applicable in each case and within their premises. - Personal data of individuals voluntarily participating in the research will be accessed only by the Member of the Consortium involved in the tasks for with the data has been collected. - Personal data of individuals voluntary participating in the research will be collected only after informed consent is given by the subject.	Risk sufficiently mitigated.

Purpose Specification Is data collected for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes?	Art 4.1 (b) Directive (EU) 2016/680 Art 5.1 (b) Regulation (EU) 2016/679	- Data collected for the purpose of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties being used for research purposes. - Data collected from participants in the research being used for purposes different from obtaining their feedback.	- Purpose has been specified and will be communicated to all partners. - All partners will receive advice from the EAB on the respect of the purpose principle. - No personal data will be used in the research and development phase of the project. - Personal data will only be used by LEAs in the course of the activities they are competent for- and in compliance with their legal framework- when testing and evaluating SPIRIT solutions. - Personal data from the participants in the research will be kept under the responsibility of the controller, in this case SPIRIT coordinator, and will not be shared or transferred to partners other than those directly involved in the evaluation of the feedback, when needed for communication purposes.	- Close monitoring of the activities involving real data will be conducted throughout the duration of the project.
Data minimisation Is the data adequate, relevant and not excessive in relation to the purposes for which they are processed? Are partners/users collecting data that is not necessary?	Art 4.1. (c) Directive (EU) 2016/680 Art 5.1 (c) Regulation (EU) 2016/679	- Collection of data from individuals' other than those investigated for a crime. - Misuse of SPIRIT crawling capabilities to collect data on individuals	- An incidental findings policy has been designed. - Real data will only be used in the phase of evaluation and not in the developing phase.	- Close monitoring of the activities involving real data will be conducted throughout the duration of the project. - Risk not completely mitigated.

		different than the suspects of crimes. - Collection of sensitive data from vulnerable or at-risk individuals.	- Only LEA officers and their staff will access real data. - Whenever a member of the project other that LEA officers and staff need to access real data this will be done by staff with the adequate level of clearance according to the national legal framework of the LEA. - Feedback from the training and evaluation processes will be given back to the SPIRIT Consortium after full anonymization. - The Ethical leader partner will review the evaluation plan of the project. - The DOW foresees ad-hoc training and awareness-raising sessions with LEA officers and/or staff taking part in the evaluation activities - The issue of possible risk of misuse beyond the project lifecycle is rightly seen as a complex challenge facing innovation in general and beyond ensuring that resulting systems will have operational audit controls that would require approval for any Variation of Use, the Consortium will endeavour to formulate safeguards in the exploitation planning stage to mitigate the risk of exposure to the results to misuse.	- Further measures will need to be implemented.

Data accuracy What processes are in place for ensuring information quality, i.e., that the information is relevant, reliable, accurate, actionable? Is there a policy or procedure in place to correct data collected?	Art. 4.1 (d) Directive (EU) 2016/680 Art 5.1 (b) Regulation (EU) 2016/679	- False positives in the information collected. - Data collected become outdated or incorrect over time.	- In order that false positives are minimised the algorithmic development will favour the statistical Type II error. - Senior Investigating Officers from LEAs involved in operational casework will conduct reviews, supported by the ontology, ensuring relevancy of data.	- Risk not completely mitigated. - Further measures will need to be implemented. - Close monitoring of the activities involving real data will be conducted throughout the duration of the project.
Data storage and retention Is data being added to databases? Is there a policy, procedure, rationale for archiving personal information? Are there procedures for reviewing how long data should be retained?	Art. 4.1 (e) Directive (EU) 2016/680 Art 5.1 (e) Regulation (EU) 2016/679	- Data being stored longer that lawful. - Data being transfer to third parties' databases. - Data from participants being kept longer than necessary. - Data from participants being transferred to databases outside the SPIRIT project.	- No personal data will be transferred from LEA evaluation exercises to SPIRIT databases. The results and feedback will be fully anonymised. - No personal data will be exchanges among the different participating LEAs except in cases allowed by their national legislations. - Personal data from voluntary participants will be erased after the end of the project. Except those data needed for auditing processes in front of the European Commission. - Data stored by LEAs will be subject to national legislation requirements and their own monitoring procedures. - Each end-user will be responsible, as controller of the personal data, to ensure the secure	- Risk sufficiently mitigated. - Close monitoring of the activities involving real data will be conducted throughout the duration of the project.

			storage and destruction of the data.	
Data security Is there a risk of information being stolen / lost / altered / rendered unavailable / system hacked? What preventative measures are in place? Are communications encrypted? What kind of encryption is used? What action will be taken if there is a data breach? Are individuals informed if their personal data is lost, stolen or other compromised? Will any other organisations be informed?	Art. 4.1 (f) Directive (EU) 2016/680 Art 5.1 (f) Regulation (EU) 2016/679	- Data being stolen/lost/altered/ rendered unavailable / system hacked. - Partners including personal data in their communications. - Personal data being included in dissemination activities or documents.	- No personal data from investigated individuals will be stored by the SPIRIT technical partners. - Before implementing SPIRIT technology in LEAs premises, they will be asked to provide information on the security systems and procedures they have in place in order to ensure that this are according to European and national standards. - No personal data from individuals will be included in communications between partners. - Anonymization will be the standard procedure in dissemination. - When a member of the Consortium detects a data breach this will be communicated immediately to the Ethical Lead Partner, the DPO and the EAB. - The Ethical Lead Partner will consult with the EAB and make a decision on the steps to take to correct/minimise the impact of the breach. - Each end-user will be responsible, as controller of the personal data, to ensure the secure storage of the data.	- Risk sufficiently mitigated. - Close monitoring of the activities involving real data will be conducted throughout the duration of the project.

Access Rights Are individuals explicitly informed about why their personal data is being collected and how it may be used? Are individuals provided with the possibility to access and correct their personal information? Can they request the deletion of some or all of their personal information? Is it necessary to restrict access to data? If so, are these restrictions adequately circumscribed and explained?	Chapter III Directive (EU) 2016/680 Chapter III Regulation (EU) 2016/679	- Access, rectification and deletion being denied to citizens. - Restriction to access rights not correctly applied.	- Access rights of individuals subject to investigation will be exercised before the relevant LEA, following the procedures defined in each national legal framework. - Access rights of participants in the research will be exercised before the coordination of the Consortium. - Participants in the research will be informed of the possibility to request correction or deletion of their personal data at any time. - In case an individual requests access to data that has been processed in the evaluation or training session and with SPIRIT platform, the LEA-controller that receives the petition shall immediately notify the IEB and the DPO so that they can evaluate if the communication of the information can pose any risks in terms of potential misuse of the research	- Risk sufficiently mitigated. - Close monitoring of the activities involving real data will be conducted throughout the duration of the project.
Accountability and monitoring Are data protection standards and procedures effectively implemented? Are oversight mechanisms in place to overview existing practices and to provide guidance to the partners of the Consortium?	Chapter IV Directive (EU) 2016/680 Chapter IV Regulation (EU)	- Misuse of the SPIRIT technology. - End-users using SPIRIT technology in a manner that is not compliant with the ethical and legal framework	- LEAs will act under their national legal frameworks and monitoring systems; however, minimum standards have already been set up by the Consortium. - An Independent Ethics Board has been set up.	- Risk not completely mitigated. - Further measures will need to be implemented. - Close monitoring of the activities involving real data will be conducted throughout the

	2016/679	- Partners acting in their own premises and applying their own practices, avoiding the oversight mechanisms in place.	- The Ethical partners will conduct periodic meetings will WP and task leaders to ensure that the activities of the project are conducted in compliance with the ethical and legal framework. - A Data Protection Officer will be set up within the Consortium. - WP leaders are responsible for the activities conducted within their WP and will consult/notify the Ethical leader partners and the IEB whenever a doubt, risk or issue appears. - The Ethical leader partner will be in contact with the DPOs and responsible staff from the different end-users. - Competent national authorities will be notified of SPIRIT activities.	duration of the project.

ANNEX 2: PRELIMINARY DPIA CONCLUSIONS

1. Levels of access and conditions have been agreed with LEAs and are included in the signed Service Contract.

2. Personal data of citizens will only be processed in the evaluation phase by members of LEAs that are controllers of such data.

3. Personal data of citizens will only be processed by LEAs according to the legal framework applicable in each case and within their premises.

4. Personal data of individuals voluntarily participating in the research will be accessed only by the Member of the Consortium involved in the tasks for with the data has been collected.

5. Personal data of individuals voluntary participating in the research will be collected only after informed consent is given by the subject.

6. Purposes of prevention, investigation, detection, and prosecution of criminal offences have been specified and will be (actually have already been) communicated to all partners. No data collected from participants in the research will be used for purposes different from obtaining their feedback.

7. All partners will receive advice from the EAB on the respect of the purpose principle.

8. No personal data will be used in the research and development phase of the project.

9. Personal data will only be used by LEAs in the course of the activities they are competent for- and in compliance with their legal framework- when testing and evaluating SPIRIT solutions.

10. Personal data from the participants in the research will be kept under the responsibility of the controller, in this case SPIRIT coordinator, and will not be shared or transferred to partners other than those directly involved in the evaluation of the feedback, when needed for communication purposes.

11. An incidental findings policy has been designed. Close monitoring of the activities involving real data will be conducted throughout the duration of the project.

12. Real data will only be used in the phase of evaluation and not in the developing phase.

13. Only LEA officers and their staff will access real data.

14. Whenever a member of the project other that LEA officers and staff need to access real data this will be done by staff with the adequate level of clearance according to the national legal framework of the LEA.

15. Feedback from the training and evaluation processes will be given back to the SPIRIT Consortium after full anonymization.

16. The Ethical leader partner will review the evaluation plan of the project.

17. The DOW foresees ad-hoc training and awareness-raising sessions with LEA officers and/or staff taking part in the evaluation activities

18. The issue of possible risk of misuse beyond the project lifecycle is rightly seen as a complex challenge facing innovation in general and beyond ensuring that resulting systems will have operational audit controls that would require approval for any Variation of Use, the Consortium will endeavour to formulate safeguards in the exploitation planning stage to mitigate the risk of exposure to the results to misuse.

19. In order that false positives are minimised the algorithmic development will favour the statistical Type II error.

20. Senior Investigating Officers from LEAs involved in operational casework will conduct reviews, supported by the ontology, ensuring relevancy of data.

21. No personal data will be transferred from LEA evaluation exercises to SPIRIT databases. The results and feedback will be fully anonymised.

22. No personal data will be exchanged among the different participating LEAs except in cases allowed by their national legislations.

23. Personal data from voluntary participants will be erased after the end of the project. Except those data needed for auditing processes in front of the European Commission.

24. Data stored by LEAs will be subject to national legislation requirements and their own monitoring procedures.

25. Each end-user will be responsible, as controller of the personal data, to ensure the secure storage and destruction of the data.

26. No personal data from investigated individuals will be stored by the SPIRIT technical partners.

27. Before implementing SPIRIT technology in LEAs premises, they will be asked to provide information on the security systems and procedures they have in place in order to ensure that this are according to European and national standards.

28. No personal data from individuals will be included in communications between partners.

29. Anonymization will be the standard procedure in dissemination.

30. When a member of the Consortium detects a data breach this will be communicated immediately to the Ethical Lead Partner, the DPO and the EAB.

31. The Ethical Lead Partner will consult with the EAB and make a decision on the steps to take to correct/minimise the impact of the breach.

32. Each end-user will be responsible, as controller of the personal data, to ensure the secure storage of the data.

33. Access rights of individuals subject to investigation will be exercised before the relevant LEA, following the procedures defined in each national legal framework.

34. Participants in the research will be informed of the possibility to request correction or deletion of their personal data at any time.

35. In case an individual requests access to data that has been processed in the evaluation or training session and with SPIRIT platform, the LEA-controller that receives the petition shall immediately notify the IEB and the DPO so that they can evaluate if the communication of the information can pose any risks in terms of potential misuse of the research.

36. LEAs will act under their national legal frameworks and monitoring systems; however, minimum standards have already been set up by the Consortium.

37. An Ethical Advisory Board has been set up.

38. The Ethical partners will conduct periodic meetings will WP and task leaders to ensure that the activities of the project are conducted in compliance with the ethical and legal framework.

39. A Data Protection Officer will be appointed within the Consortium.

40. WP leaders are responsible for the activities conducted within their WP and will consult/notify the Ethical leader partners and the IEB whenever a doubt, risk or issue appears.

41. The Ethical leader partner will be in contact with the DPOs and responsible staff from the different end-users.

42. Competent national authorities will be notified of SPIRIT activities.

ANNEX 3: Consultation-UAB. Incidental Findings Policy-SPIRIT End-users (LEA)

ID 11	STAD ANTWERPEN. Belgium
ID 12	WYZSZA SZKOLA POLICJI W SZCZYTNIE. Poland
ID 13	WEST MIDLANDS POLICE AUTHORITY. United Kingdom
ID 14	THAMES VALLEY POLICE. United Kingdom
ID 15	MINISTARSTVO UNUTRASNJIH POSLOVA REPUBLIKE SRBIJE. Serbia
ID 16	HELLENIC POLICE. Greece

User ID_____

Introduction

The aim of this consultation is to ask from SPIRIT end-users for relevant information related to incidental findings policies. An incidental finding is defined as any information gathered during an ongoing investigation which is not related to the purpose of the investigation but that may affect or jeopardize the individual rights of citizens who are innocent or might not be involved in the investigation.

Consultation

1. Does your organisation have any specific internal protocols, guidelines, or best practices in order to handle incidental findings?

   - Yes
   - No

2. If yes, are these internal protocols, guidelines or best practices related to incidental findings described in a specific document?.

- Yes
- No

3. If the Incidental Findings policy is described in a document, is this document publicly available?
   - Yes
   - No

4. If these internal protocols, guidelines or best practices related to incidental findings are not described in a document, could you provide some information regarding your procedures when an incidental finding occurs? What do you do in these situations?

ANNEX 4: LEA'S ORIGINAL ANSWERS. Consultation-UAB.

ID 11	STAD ANTWERPEN. Belgium

1. Does your organisation have any specific internal protocols, guidelines, or best practices in order to handle incidental findings?

☐ Yes
x No

2. If yes, are these internal protocols, guidelines or best practices related to incidental findings described in a specific document?

☐ Yes, they are described in a document
☐ No, but we are aware of the existence of this incidental finding policy

3. If the Incidental Findings policy is described in a document, is this document publicly available?

☐ Yes
☐ No

4. If these internal protocols, guidelines or best practices related to incidental findings are not described in a document, could you provide some information regarding your procedures when an incidental finding occurs? What do you do in these situations?

ID12	WYZSZA SZKOLA POLICJI W SZCZYTNIE. Poland

1. Does your organisation have any specific internal protocols, guidelines, or best practices in order to handle incidental findings?

☐ Yes

☐ No

2. If yes, are these internal protocols, guidelines or best practices related to incidental findings described in a specific document?

☐ Yes, they are described in a document

☐ No, but we are aware of the existence of this incidental finding policy

3. If the Incidental Findings policy is described in a document, is this document publicly available?

☐ Yes

☐ No

4. If these internal protocols, guidelines or best practices related to incidental findings are not described in a document, could you provide some information regarding your procedures when an incidental finding occurs? What do you do in these situations?

For clarification:

E-mail to Emma Teodoro, 10/10/2018

Our internal protocols, guidelines and good practices related to incidental findings are described in several different documents. These are specific regulations of individual acts of law. Among others, they are included in the Police Act, the Code of Criminal Procedure and internal police law regulations governing the conduct of investigations and classified police activities. These specific regulations determine the way of proceeding with obtaining information about a person, its action (legal or illegal) or about a situation, an event or a crime. Of course, all the regulations regarding respect for human, civil and personal rights and the protection of sensitive information are also applicable.

The general rule is that if we obtain information about the crime or criminals that indicate to a direct threat to human life and health, appropriate and adequate actions will be taken.

If the information relates simply to another offense, it may be the basis for initiating a separate investigation. The condition is to carry it out completely and establish other evidences confirming crime conduct and the guilt of a specific person. When it comes to interviewing people and making statements in the investigation, we have, of course, specific regulations, rights for a witness or a suspect, about which we are obliged to warn persons before starting an activity. These regulations indicate that the witness may refuse to answer the question if the answer would involve criminal liability for him or for the closest person. The suspect has the

general right to refuse to provide explanations or answers to specific questions. These are obvious procedural guarantees that are to secure the rights of individuals to avoid self-incrimination.

Police officers are obliged to respect the protection of all kinds of secrets: state, official, correspondence, journalistic, medical, insurance or other types of secrecy specified in the law. Access to them results from certain powers of the police and is always carried out as part of the investigation and in connection with it, always in justified need and circumstances. The specified procedure is always then applied, registered and approved by the prosecution or the court. If the police incidentally get access to such information, for example through people or situational reasons, for example due to inappropriate protection or unlawful disclosure, it is also obliged to guard the secret and follow the procedures.

If we obtain any sensitive information about a particular person who is the subject of an investigation or about other persons who are not subject of an investigation, then of course they cannot be the subject of our proceedings or be transferred to other institutions or offices.

In summary, there is a wide variety of regulations that guarantee the protection of information and people and against police activities that may harm human and civil rights. Special attention is paid to the right to protection of sensitive information and there is a great awareness of respecting the privacy of human intimacy. Of course, we are aware that the work of the police concerns various spheres of human existence and activity. We know how often very private information are obtained and we deal with them extremely carefully. Everything to respect every human being.

ID 13	WEST MIDLANDS POLICE AUTHORITY. United Kingdom

1. Does your organisation have any specific internal protocols, guidelines, or best practices in order to handle incidental findings?

☒ Yes
☐ No

2. If yes, are these internal protocols, guidelines or best practices related to incidental findings described in a specific document?

☒ Yes, they are described in a document
☐ No, but we are aware of the existence of this incidental finding policy

3. If the Incidental Findings policy is described in a document, is this document publicly available?

☒ Yes
☐ No

4. If these internal protocols, guidelines or best practices related to incidental findings are not described in a document, could you provide some information regarding your procedures when an incidental finding occurs? What do you do in these situations?
5. ---Incidental findings are catered for by legislation. This places a positive obligation on all police officers to retain, review and make available all material obtained during an investigation. –

The legislation is called the Criminal Procedure and Investigation Act 1996----------

There is no opt out to this procedure and all material is subject of a review both internally and by a reviewing lawyer.----------

ID 14	THAMES VALLEY POLICE. United Kingdom

1. Does your organisation have any specific internal protocols, guidelines, or best practices in order to handle incidental findings?

■ Yes
☐ No

2. If yes, are these internal protocols, guidelines or best practices related to incidental findings described in a specific document?

■ Yes, they are described in a document
☐ No, but we are aware of the existence of this incidental finding policy

3. If the Incidental Findings policy is described in a document, is this document publicly available?

■ Yes
☐ No

4. If these internal protocols, guidelines or best practices related to incidental findings are not described in a document, could you provide some information regarding your procedures when an incidental finding occurs? What do you do in these situations?

This information is not held in one specific document, there are different processes and policy for different areas of work which will factor in collateral intrusion.

An example of this is RIPA /IPA Regulation of Investigatory Powers Act 2000/Investigatory Powers Act

MOPI -Management of Police Information.

OPT (Operational Partner Team) Prisons.

ID 15	MINISTARSTVO UNUTRASNJIH POSLOVA REPUBLIKE SRBIJE. Serbia

1. Does your organisation have any specific internal protocols, guidelines, or best practices in order to handle incidental findings?

☐ Yes
☒ No

2. If yes, are these internal protocols, guidelines or best practices related to incidental findings described in a specific document?

☐ Yes, they are described in a document
☐ No, but we are aware of the existence of this incidental finding policy

3. If the Incidental Findings policy is described in a document, is this document publicly available?

☐ Yes
☐ No

4. If these internal protocols, guidelines or best practices related to incidental findings are not described in a document, could you provide some information regarding your procedures when an incidental finding occurs? What do you do in these situations?

Law on personal data protection tell us that:
"The processing of personal data is not allowed if the data being processed is unnecessary or inappropriate for the purpose of processing."
This law does not tell us what to do with such data, so we remove them (delete them) for practical reasons (due to the space on the memory devices).
The Commissioner for the Protection of personal information may order the deletion of data, but only if they are unlawfully collected, not if they have no relation to the purpose of investigation.
All data my service collects are classified by the degree of secrecy - strictly confidential, the law that protects such data is much more restrictive.

European Commission | Horizon 2020 European Union funding for Research & Innovation

Project funded by H2020 Programme – Grant Agreement number: 786993

ID 16	HELLENIC POLICE. Greece

Questionnaire

1. Does your organisation have any specific internal protocols, guidelines, or best practices in order to handle incidental findings?

   X Yes
   ☐ No

2. If yes, are these internal protocols, guidelines or best practices related to incidental findings described in a specific document?

   X Yes, they are described in a document
   ☐ No, but we are aware of the existence of this incidental finding policy

3. If the Incidental Findings policy is described in a document, is this document publicly available?

   ☐ Yes
   X No

4. If these internal protocols, guidelines or best practices related to incidental findings are not described in a document, could you provide some information regarding your procedures when an incidental finding occurs? What do you do in these situations?

If during an ongoing investigation an incidental finding is occurred, this finding is most likely that will fall within a certain area of competence, for which internal protocols, guidelines or best practices would exist.

European Commission | Horizon 2020 European Union funding for Research & Innovation

Project funded by H2020 Programme – Grant Agreement number: 786993

ANNEX 5: Intended Survey. Questionnaire-UAB. Incidental Findings Policy-Spirit End-users (LEA) [to be discussed with the EAB]

Introduction

The aim of this questionnaire is to collect from SPIRIT end-users relevant information related to incidental findings policies. An incidental finding is defined as any information gathered during an ongoing investigation which is not related to the purpose of the investigation but that may affect or jeopardize the individual rights of citizens who are innocent or might not be involved in the investigation. The questions are grouped by source, following the categories in the risk model. Due to the sensitive and confidential nature of such a questioning, it will be submitted and discussed with the EAB and with LEAs' representatives.

LEAs' responses to the questionnaire cannot be provided without a common work-in-progress and an appropriate research framework. Hence, they will be elicited within a specific Workshop with LEAs' investigators and, eventually, controllers (DPOs). They will be formulated after after all internal and external permits have been duly signed and protections (informed consent) have been put in place. We will use the focus group techniques.

Survey (questionnaire, confidential)

Please insert your User ID according to the following table:

ID 11	STAD ANTWERPEN. Belgium
ID 12	WYZSZA SZKOLA POLICJI W SZCZYTNIE. Poland
ID 13	WEST MIDLANDS POLICE AUTHORITY. United Kingdom
ID 14	THAMES VALLEY POLICE. United Kingdom
ID 15	MINISTARSTVO UNUTRASNJIH POSLOVA REPUBLIKE SRBIJE. Serbia
ID 16	HELLENIC POLICE. Greece

User ID_____

European Commission | Horizon 2020 European Union funding for Research & Innovation

Project funded by H2020 Programme – Grant Agreement number: 786993

Please supply the information requested and answer the questions as needed.

1. Personnel Management
a. Management of incentives

Salary structures and bonus systems for all officers and other staff (at all levels) who will use the system
Do you think the system will help officers to do their jobs better?
Will this be rewarded by promotion, recognition, salary increases or bonuses?
Do you have existing disciplinary arrangements related to misuse of data?
Has guidance been issued to staff about privacy and confidentiality, treatment of witnesses, suspects, arrested individuals?

b. Corruption + selling access to data
Reports from inquiries into police corruption during the last ten years
Details of enquiries/procedures into misuse of position by staff during the last ten years
Any ongoing investigations into corruption
Do you think there are any such problems in your country? How prevalent is this?

c. Vendettas against groups or individuals
Press reports about police bias
Which groups do you think may be targeted? By whom?
Complaints data from groups or individuals

d. Deals with contacts in criminal-commercial organisations
Is it possible that relationships with criminal or commercial organisations may adversely affect attitudes to use of personal data?
Have you had any problems over the exchange of personal information recently?
Have there been any enquiries into such issues in your country in the last ten years?

e. Practical and Procedural matters
How difficult do you find it to recruit well-qualified staff?
Details of internal and external training programmes with respect to privacy and confidentiality
How much supervision do junior staff get when handling personal data?
How do officers log in to their computers at present?
What security systems do you use? Password? Facial recognition? Fingerprints?

f. Embedded practices, legacy systems
How do you currently investigate persons of interest?
Do you explore social media such as Facebook and Twitter?
How do you access such data?
Are the computers and laptops you use up-to-date with anti-virus and other security systems?

2. LEAs
a. Inadequate management
Are all the management positions in your organisation currently staffed?

Would you say that your management is efficient and organised?
Do all lower-level staff get adequate supervision?

b. Weak governance
Annual reports, both publicly available and internal, for the last five years.
Please give details of your governance structure, including lines of reporting.
Do you have a Board of Governors? Does it have a Charter, or a Code of Conduct?
Have there been any enquiries into the management or governance of any LEAs in your country in the last ten years?

c. Lack of accountability
When officers make mistakes in your organisation, what happens next?
Are there any staff appeal processes?
Do you have any Whistleblower protections in place?

d. Relationships with other agencies
Do you share data with any other government or non-government agencies?
If so, what procedures are in place to monitor their use of your data?
Is the sharing of data explicitly required or provided by law?
Are you concerned about the trustworthiness of any of the agencies with which you deal?
Do you think that their accountability and compliance processes are adequate?

e. Inter-departmental rivalries
Who would you say are your main rivals within the security or governmental system?
Do you have a friendly and professional relationship with them?
Do you think these rivalries impact on privacy and confidentiality?

3. Political
a. Electoral gerrymandering
Report of electoral commission into elections during the last ten years
Do you trust the politicians in your country to stick by the rules during elections?
Have there been recent instances of politicians misusing personal or other data during election times in order to gain political advantage?

b. Vendettas against groups - eg Jews, migrants
Are there any political groups in your country who express hate or otherwise deride particular groups?
How powerful are such groups?
Has there been any recent evidence of these groups misusing data on individuals in order to pursue vendettas against particular individuals or groups of individuals?

c. Discriminatory policies, bias
Reports Commissions again sex, race or other discrimination
Does your country have anti-discriminatory policies and procedures in addition to those at EU level?
Would you say that your current government's policies with respect to sex, race or religious discrimination are robust?

Project funded by H2020 Programme – Grant Agreement number: 786993

d. Damaging political opponents

Have there been any instances of the misuse of data by politicians to discredit opponents in the last ten years?

Are you aware of any press reports of such activities?

e. Finding scapegoats

Do you think that your government seeks to deflect blame for failed policies?

Can you provide a recent example? Did it involve an individual or a group?

4. External

a. Professional hackers

Have there been any instances of LEA systems that have been hacked in the last ten years?

Are you aware of any professional groups operating in your country?

Have there been any inquiries into the operations of such groups? If so, can we have their reports?

b. Foreign governments - eg China, Russia

Has there been any concern in the last five years about foreign governments seeking to access citizen's or public agencies' data?

If so, how have they obtained such data? Through hacking?

Are there any countries you are particularly concerned about?

What counter-measures do you have in place to prevent such attacks?

c. Blackmail of officials

Have there been any cases where officials have been found to face undue pressure from external groups?

Have there been any enquiries into such problems in the last ten years?

d. Dark Web

Do you think the Dark Web constitutes a threat to privacy and the security of data?

Have there been any examples of data being sold on the Dark Web. If so, can we have details?

To your knowledge, how many interactions do you think are criminal in the dark web?

e. Virus-ransomware

What security arrangements do you have in place on your networks, and on laptops, computers and phones, to prevent virus or ransomware attacks?

Would you say that these systems are state-of-the-art?

f. Bankruptcy-failure of operating company

Financial statements of proposed operating company for last five years.

Press reports on the company, including any recent changes of senior management.

Due diligence enquiries into the company.

5. Reputational attacks (by press etc?)

a. Highlighting of system failures

Are you aware of any groups that may seek to attack your use of the system?

Is there any previous evidence of such attacks?
How prevalent would you say is dissatisfaction with your LEAs treatment of privacy and data security issues?
Are there any particular journalists who highlight such issues?

b. Lobbyists

How many lobbyist groups operate in your country on privacy and data-related issues?
How well resourced and respected are they?
If possible, please provide links to their webpages etc.

c. Technological failures

How robust are your networks and computer systems?
Have there been any failures in the last five years?
Could these past failures be used by others to discredit your use of the system?

ANNEX 6: Example of License (Sample: to be discussed, agreed and adapted to Data Protection requirements within the SPIRIT Consortium)

Apache License, Version 2.0 Apache License Version 2.0, January 2004 http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License.

Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License.

Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution.

You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

You must give any other recipients of the Work or Derivative Works a copy of this License; and You must cause any modified files to carry prominent notices stating that You changed the files; and You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License. You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions.

Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks.

This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty.

Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability.

In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability.

While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

APPENDIX: How to apply the Apache License to your work

To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets "[]" replaced with your own identifying information. (Don't include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same "printed page" as the copyright notice for easier identification within third-party archives.

Copyright [yyyy] [name of copyright owner]

Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at

http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

ANNEX 7: EAB Approval

SPIRIT
© 2018 SPIRIT ALL RIGHTS RESERVED

Monday 29th October 2018

TO WHOM IT MAY CONCERN

Dear Sir/Madam

EUROPEAN UNION SPIRIT PROJECT

I hereby declare that I have read, and I accept the outcomes of the deliverables foreseen for M3 carried out in the European Union SPIRIT Project, including docs D9.1 on the Informed Consent, D9.2 on the Incidental Findings, D9.3 on the Ethics Advisory Board and D9.4 on Notification to National Data Protection Authorities.

The Project has successfully completed this round of deliverables in strict accordance with rules and principles of the General Data Protection Regulation (EU) 2018/679 (GDPR) and Directive (EU) 2016/680.

Please let me know if I can be of further assistance.

Yours sincerely,

Ugo Pagallo
Professor of Jurisprudence at the Department of Law,
University of Turin,
Turin, Italy

SPIRIT

Monday 29th October 2018

TO WHOM IT MAY CONCERN

Dear Sir/Madam

EUROPEAN UNION SPIRIT PROJECT

I hereby declare that I have read, and I accept the outcomes of the deliverables foreseen for M3 carried out in the European Union SPIRIT Project, including docs D9.1 on the Informed Consent, D9.2 on the Incidental Findings, D9.3 on the Ethics Advisory Board and D9.4 on Notification to National Data Protection Authorities.

The Project has successfully completed this round of deliverables in strict accordance with rules and principles of the General Data Protection Regulation (EU) 2018/679 (GDPR) and Directive (EU) 2016/680.

Please let me know if I can be of further assistance.

Yours sincerely,

Lilian Mitrou
Professor at Department of Information and
Communication System Engineering,
University of the Aegean, Greece

European Commission | Horizon 2020 European Union funding for Research & Innovation

Project funded by H2020 Programme – Grant Agreement number: 786993

SPIRIT

Monday 29th October 2018

TO WHOM IT MAY CONCERN

Dear Sir/Madam

EUROPEAN UNION SPIRIT PROJECT

I hereby declare that I have read, and I accept the outcomes of the deliverables foreseen for M3 carried out in the European Union SPIRIT Project, including docs D9.1 on the Informed Consent, D9.2 on the Incidental Findings, D9.3 on the Ethics Advisory Board and D9.4 on Notification to National Data Protection Authorities.

The Project has successfully completed this round of deliverables in strict accordance with rules and principles of the General Data Protection Regulation (EU) 2018/679 (GDPR) and Directive (EU) 2016/680.

Please let me know if I can be of further assistance.

Yours sincerely,

Virginia Dignum
Full Professor at Department of Computing Science,
Umeå universitet, Sweden

European Commission | Horizon 2020 European Union funding for Research & Innovation

Project funded by H2020 Programme – Grant Agreement number: 786993

SPIRIT

Monday 29th October 2018

TO WHOM IT MAY CONCERN

Dear Sir/Madam

EUROPEAN UNION SPIRIT PROJECT

I hereby declare that I have read, and I accept the outcomes of the deliverables foreseen for M3 carried out in the European Union SPIRIT Project, including docs D9.1 on the Informed Consent, D9.2 on the Incidental Findings, D9.3 on the Ethics Advisory Board and D9.4 on Notification to National Data Protection Authorities.

The Project has successfully completed this round of deliverables in strict accordance with rules and principles of the General Data Protection Regulation (EU) 2018/679 (GDPR) and Directive (EU) 2016/680.

Please let me know if I can be of further assistance.

Yours sincerely,

David Watts
Professor of Information Law and Policy
La Trobe Law School,
La Trobe University, Australia

European Commission | Horizon 2020 European Union funding for Research & Innovation

Project funded by H2020 Programme – Grant Agreement number: 786993

SPIRIT

Monday 29th October 2018

TO WHOM IT MAY CONCERN

Dear Sir/Madam

EUROPEAN UNION SPIRIT PROJECT

I hereby declare that I have read, and I accept the outcomes of the deliverables foreseen for M3 carried out in the European Union SPIRIT Project, including docs D9.1 on the Informed Consent, D9.2 on the Incidental Findings, D9.3 on the Ethics Advisory Board and D9.4 on Notification to National Data Protection Authorities.

The Project has successfully completed this round of deliverables in strict accordance with rules and principles of the General Data Protection Regulation (EU) 2018/679 (GDPR) and Directive (EU) 2016/680.

Please let me know if I can be of further assistance.

Yours sincerely,

Giovanni Sartor

Giovanni Sartor
Full Professor in Legal Informatics-Computers and Law
at University of Bologna,
Bologna, Italy

European Commission | Horizon 2020 European Union funding for Research & Innovation

Project funded by H2020 Programme – Grant Agreement number: 786993

ANNEX 8: Replies to the UAB Questionnaire

REPLY 1

QUESTIONNAIRE

Data and information to establish possible magnitude of incidental and residual risks

Please supply the following information and answer the following questions:

Incidental Risks – by Source and Category

1. Individuals
    a. Use for personal career advancement

Do you think the system will help officers to do their jobs better? Yes, by allowing for the quicker and more accurate establishment of the true identity of a suspect.
Will this be rewarded by promotion, recognition, salary increases or bonuses? No
Disciplinary arrangements for officers, including any related to misuse of data None – protective monitoring capability in place, supported by system audit capabilities.
Details of enquiries/procedures into misuse of position by staff during the last ten years There are a number of ongoing investigations into police misconduct at any one time; occasionally this relates to computer misuse and results in the officer or staff member being disciplined, which can include dismissal. I am confident that we have a proven process to uncover such issues and deal with the ramifications.
Guidance issued to staff about privacy and confidentiality, treatment of witnesses, suspects, arrested individuals Yes, via vetting procedure, HR induction, operational guidance, IT security management policy, Information Management policy; these policies are available via the Force internet service.

    b. Corruption + selling access to data

Do you think there are any such problems in your country? How prevalent is this? There is always a potential, but no evidence of this occurring recently
Reports from inquiries into police corruption during the last ten years These are not generally disclosable, but IOPC do publish findings; all corruption/misconduct summaries are published in force
Any ongoing investigations into corruption Yes, but not related to data integrity relating to specialist intelligence teams.

    c. Vendettas against groups or individuals

Press reports about police bias – All managers are trained to deal with conscious and unconscious bias; although there are nationally reports of police bias, the force is not currently subject of such allegations
Which groups do you think may be targeted? By whom? There is no identified group
Complaints data from groups or individuals This question is not specific enough to answer

    d. Deals with contacts in criminal-commercial organisations

Have there been allegations about relationships with criminal or commercial organisations? No, we have a disclosable associations policy that supports vetting to uncover any such associations, with allegations being investigated by the Counter Corruption Unit
Did any of these involve exchange of sensitive information? N/A

Have there been any enquiries into such issues in your country in the last ten years? Probably….

e. Mistakes, incompetence, inattention

How difficult do you find it to recruit well-qualified staff? We take suitable candidates and train them to meet our needs.
Details of internal and external training programmes with respect to use of data Mandatory training for all staff through NCALT and Moodle for the likes of GDPR, MOPI, Disclosure etc; role specific training for applications
How much supervision do junior staff get when handling personal data? As above, supported by mentoring and coaching
Details of all relevant disciplinary hearings in the last ten years N/A
How do officers log in to their computers at present? Using a personal identification and password combination, which is routinely changed and consists of various characters
What security systems do you use? Password? Facial recognition? Fingerprints? As above

f. Embedded practices, legacy systems

How do you currently investigate persons of interest? Through use of Police and third party IT systems to build a profile
Do you explore social media such as Facebook and Twitter? Yes
How do you access such data? Through overt and covert accounts
Are the computers and laptops you use up-to-date with anti-virus and other security systems? Yes

2. LEAs

a. Inadequate management

Are all the management positions in your organisation currently staffed? Yes
Would you say that your management is efficient and organised? Yes
Do all lower-level staff get adequate supervision? Yes

b. Weak governance

Annual reports for the last five years.
Please give details of your governance structure, including lines of reporting. Governance is provided via HMIC, Service Improvement (Audit and interview) and Peer assessment
Do you have a Board of Governors? Does it have a Charter, or a Code of Conduct? Overall governance is provided via the PCC and through misconduct processes (professional Standards department , IOPC and Misconduct Panel)
Have there been any enquiries into the management or governance of any LEAs in your country in the last ten years? This question is too open to answer

c. Lack of accountability

When officers make mistakes in your organisation, what happens next? Debrief to establish any ongoing threat, harm or risk, followed by consideration of misconduct and individual and organisational learning
Are there any staff appeal processes? Yes
Do you have any Whistleblower protections in place? Yes, plus an Integrity Line

d. Relationships with other agencies

Do you share data with any other government or non-government agencies? Yes, under data sharing agreements
If so, what procedures are in place to monitor their use of your data? The data is shared under conditional use, which is generally governed through the individual agencies own processes as a data processor. Intelligence is governed by it's own information handling conditions
Are you concerned about the trustworthiness of any of the agencies with which you deal? No

e. Inter-departmental rivalries

Who would you say are your main rivals within the security or governmental system? None
Do you have a friendly and professional relationship with them? N/A
Have there been instances in the last ten years where they have sought to undermine your authority or that of your organisation? N/A

3. Political

a. Electoral gerrymandering

Report of electoral commission into elections during the last ten years None
Do you trust the politicians in your country to stick by the rules during elections? They are heavily regulated by the Electoral Commission
Have there been recent instances of politicians misusing personal or other data during election times? Not within the UK, although a UK company, Cambridge Analytica were involved in the US Election

b. Vendettas against groups - eg Jews, migrants

Are there any political groups in your country who express hate or otherwise deride particular groups? We have an active left and right wing within our main political parties, extremist views are subject of sanction and prohibition. There is no evidence of any vendetta against political groups.
How powerful are such groups? limited
Has there been any recent evidence of these groups misusing data on individuals? No

c. Discriminatory policies, bias

Reports of sex, race or other Commissions Nationally, race relations can be fragile at times, there is legislation to reduce hate crime and discrimination around the strands of diversity, with equality being a key aim at national and local levels. We have such policies that are actively enforced as well as inclusion policies.
Does your country have anti-discriminatory policies and procedures in addition to those at EU level? Not sure
Would you say that your current government's policies with respect to sex, race or religious discrimination are robust? Yes

d. Damaging political opponents

Have there been any instances of the misuse of data by politicians to discredit opponents in the last ten years? No, the sanctions would be severe (see 3a above)
Are you aware of any press reports of such activities? No

e. Finding scapegoats

Do you think that your government seeks to deflect blame for failed policies? No more than any other government
Can you provide a recent example? Did it involve an individual or a group? No

4. External

a. Professional hackers

Have there been any instances of LEA systems that have been hacked in the last ten years? No
Are you aware of any professional groups operating in your country? Not personally, although there are reports of Russian, Chinese, North Korean and Iranian backed hackers working against the British interest
Have there been any inquiries into the operations of such groups? If so, can we have their reports? N/A

b. Foreign governments - eg China, Russia

Has there been any concern in the last five years about foreign governments seeking to access your data? Not to our data directly
Are there any countries you are particularly concerned about? Russian, Chinese, North Korean and Iranian
What counter-measures do you have in place to prevent such attacks? UK Government security conditions, Firewalls, secure email, escalation to UK Government Counter-Cyber capabilities

c. Blackmail of officials

Have there been any cases where officials have been found to face undue pressure from external groups? Not locally, vetting identifies potential risks, which are continually monitored
Have there been any enquiries into such problems in the last ten years? Not that I am aware of

d. Dark Web

Do you think the Dark Web constitutes a threat to privacy and the security of data? No
Have there been any examples of data being sold on the Dark Web. If so, can we have details? Not that I am aware of; there are national groups who monitor this on behalf of UK Policing (National Police Risk information Management Team)

e. Virus-ransomware

What security arrangements do you have in place on your networks, and on laptops, computers and phones, to prevent virus or ransomware attacks? Full security protocol, managed by our ICT department
Would you say that these systems are state-of-the-art? No, but have proved sufficient and security is always prioritised over convenience

f. Bankruptcy-failure of operating company

Financial statements of proposed operating company for last five years. N/A
Press reports on the company, including any recent changes of senior management. N/A
Due diligence enquiries into the company. N/A

5. Reputational attacks (by press etc?)

a. Highlighting of system failures

Are you aware of any groups that may seek to attack your use of the system? No
Is there any previous evidence of such attacks? No
How prevalent would you say is dissatisfaction with your LEAs treatment of privacy and data security issues? limited
Are there any particular journalists who highlight such issues? Not that I am aware of

b. Lobbyists

How many lobbyist groups operate in your country on privacy and data-related issues? Unknown, but we have an active civil liberties sector
How well resourced and respected are they? There appear to be well organised and funded

Project funded by H2020 Programme – Grant Agreement number: 786993

If possible, please provide links to their webpages etc.

c. Technological failures

How robust are your networks and computer systems? We work on older software and hardware to ensure security of our wider systems
Have there been any failures in the last five years? Yes
Could these past failures be used by others to discredit your use of the system? UK Policing systems are fragmented; there is a general understanding that most governmental IT is poor.

REPLY 2

QUESTIONNAIRE

Data and information to establish possible magnitude of incidental and residual risks

Please supply the following information and answer the following questions:

Incidental Risks – by Source and Category

1. Individuals
   a. Use for personal career advancement

Do you think the system will help officers to do their jobs better? Unsure at this stage. If the end system has the capability we have previously discussed then arguably yes. If capability is reduced then there is the likelihood that the systems we currently have access to will be more productive than this.

Will this be rewarded by promotion, recognition, salary increases or bonuses?
No.

Disciplinary arrangements for officers, including any related to misuse of data
There are disciplinary arrangements in place for all individuals engaged in activity on behalf WMP ROCU through the lead force of WMP. There are a variety of means for this from informal management to criminal prosecution using legislated powers.

Details of enquiries/procedures into misuse of position by staff during the last ten years
Unable to provide a response.

Guidance issued to staff about privacy and confidentiality, treatment of witnesses, suspects, arrested individuals
Variety of training both in person and electronic is provided to staff in relation to the above areas. UK Legislation provides the following safeguards:

Human Rights Act 1998 – Overarching legislation dealing with rights of the individual

Privacy and Confidentiality - Data Protection Act 2018 incorporating General Data Protection Regulations, Government Security Classification, Official Secrets Act 1989

Treatment of witnesses – Code of Practice for Victims (under Domestic Violence, Crime and Victims Act 2004), Police and Criminal Evidence Act 1984 (Witnesses, procedures for handling identification evidence and admissibility of evidence)

Suspects and Arrested Individuals – Police and Criminal Evidence Act 1984 and Serious Organised Crime Police Act 2005

European Commission | Horizon 2020 European Union funding for Research & Innovation

Project funded by H2020 Programme – Grant Agreement number: 786993

b. Corruption + selling access to data

Do you think there are any such problems in your country? How prevalent is this? Details accessible through following link: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/769403/6.5128_Anti-Corruption_Strategy_Year1_Update_v7_WEB.PDF

Reports from inquiries into police corruption during the last ten years

Information available through Independent Office for Police Conduct: https://policeconduct.gov.uk & https://www.gov.uk/government/publications/corruption-in-the-police-service-in-england-and-wales-second-report

Any ongoing investigations into corruption

Unable to provide a response.

c. Vendettas against groups or individuals

Press reports about police bias

Variety of reports in relation to police bias within the media targeting wide range of protected characteristics.

Which groups do you think may be targeted? By whom?

Unable to provide a response

Complaints data from groups or individuals

Information available through Independent Office for Police Conduct: https://policeconduct.gov.uk

d. Deals with contacts in criminal-commercial organisations

Have there been allegations about relationships with criminal or commercial organisations? Unable to provide a response

Did any of these involve exchange of sensitive information? Unable to provide a response

Have there been any enquiries into such issues in your country in the last ten years? Unable to provide a response

e. Mistakes, incompetence, inattention

How difficult do you find it to recruit well-qualified staff? Clear recruitment process in place for both police and specialised unit within the ROCU network. There are some challenges faced with recruiting and retaining technically competent staff, particularly from the commercial sector.

Details of internal and external training programmes with respect to use of data

Majority of training is delivered through National Centre for Applied Learning Technologies (NCALT)

How much supervision do junior staff get when handling personal data?

Limited – organisation handles significant amount of personal data on a daily basis. Majority is stored within layered systems and level of access depends on the role they perform within the organisation. They will have access to intelligence systems containing significant amount of personal data.

Details of all relevant disciplinary hearings in the last ten years

https://west-midlands.police.uk/misconduct-hearing-outcomes
https://www.policeconduct.gov.uk/tags/west-midlands-police

How do officers log in to their computers at present?

Yes – individual identification and authentication required in order to access all force systems and buildings.

What security systems do you use? Password? Facial recognition? Fingerprints?
Pin Card and Pin – Username and Password for some offline systems.

f. Embedded practices, legacy systems

How do you currently investigate persons of interest?
Variety of different means.

Do you explore social media such as Facebook and Twitter?
Yes

How do you access such data?
Overtly and Covertly

Are the computers and laptops you use up-to-date with anti-virus and other security systems?
Yes – all have anti-virus and encryption

2. LEAs

a. Inadequate management

Are all the management positions in your organisation currently staffed?
Yes
Would you say that your management is efficient and organised?
Yes
Do all lower-level staff get adequate supervision?
Yes

b. Weak governance

Annual reports for the last five years.
https://www.westmidlands-pcc.gov.uk/transparency/about-the-office-of-the-west-midlands-police-and-crime-commissioner/annual-reports

Please give details of your governance structure, including lines of reporting.
Hierarchical governance structure – fairly detailed structure is available if required

Do you have a Board of Governors? Does it have a Charter, or a Code of Conduct?
Responsible to 4 Police and Crime Commissioners and 4 Chief Constables
There is a national Police Code of Ethics: https://www.college.police.uk/What-we-do/Ethics/Pages/archive_DO_NOT_DELETE/Code-of-Ethics.aspx

Have there been any enquiries into the management or governance of any LEAs in your country in the last ten years?
Yes - Information available through Independent Office for Police Conduct: https://policeconduct.gov.uk

c. Lack of accountability

When officers make mistakes in your organisation, what happens next?

Depending on the nature of the incident this can be dealt with through a variety of informal and formal options. If it is a genuine mistake this is likely to take the form of words of advice.

Are there any staff appeal processes?
Yes

Do you have any Whistleblower protections in place?
Yes – required by Public Interest Disclosure Act 1998

d. Relationships with other agencies

Do you share data with any other government or non-government agencies?
Yes

If so, what procedures are in place to monitor their use of your data?
Statutory requirement to shared data in certain circumstances. Safeguards with regarding monitoring use of data differ from organisation to organisation.

Are you concerned about the trustworthiness of any of the agencies with which you deal?
No

e. Inter-departmental rivalries

Who would you say are your main rivals within the security or governmental system?
National Crime Agency (NCA), UK Intelligence Community (UKIC), Home Office Police Forces

Do you have a friendly and professional relationship with them?
Yes

Have there been instances in the last ten years where they have sought to undermine your authority or that of your organisation?
No

3. Political

a. Electoral gerrymandering

Report of electoral commission into elections during the last ten years
Information available at: https://www.electoralcommission.org.uk/our-work/publications

Do you trust the politicians in your country to stick by the rules during elections?
Yes

Have there been recent instances of politicians misusing personal or other data during election times?
Yes

b. Vendettas against groups - eg Jews, migrants

Are there any political groups in your country who express hate or otherwise deride particular groups?
Yes

How powerful are such groups?
Growing voice arguably as a consequence of ongoing Brexit issues

Has there been any recent evidence of these groups misusing data on individuals?
No

c. Discriminatory policies, bias

Reports of sex, race or other Commissions
https://www.equalityhumanrights.com/en

Does your country have anti-discriminatory policies and procedures in addition to those at EU level?
Yes – Equality Act 2010

Would you say that your current government's policies with respect to sex, race or religious discrimination are robust?
Yes

d. Damaging political opponents

Have there been any instances of the misuse of data by politicians to discredit opponents in the last ten years?
Yes

Are you aware of any press reports of such activities?
Yes

e. Finding scapegoats

Do you think that your government seeks to deflect blame for failed policies?
Yes

Can you provide a recent example? Did it involve an individual or a group?
https://www.theguardian.com/society/2016/aug/19/sharon-shoesmith-baby-p-haringey-social-services-interview

4. External

a. Professional hackers

Have there been any instances of LEA systems that have been hacked in the last ten years?
Yes

Are you aware of any professional groups operating in your country?
Yes

Have there been any inquiries into the operations of such groups? If so, can we have their reports?
Yes – no

b. Foreign governments - eg China, Russia

Has there been any concern in the last five years about foreign governments seeking to access your data?
Yes

Are there any countries you are particularly concerned about?
China / Russia / North Korea / Iran

What counter-measures do you have in place to prevent such attacks?
Unable to comment

c. Blackmail of officials

Have there been any cases where officials have been found to face undue pressure from external groups?
Yes

Have there been any enquiries into such problems in the last ten years?
Unable to comment

d. Dark Web

Do you think the Dark Web constitutes a threat to privacy and the security of data?
Yes

Have there been any examples of data being sold on the Dark Web. If so, can we have details?
Yes – basic Google search will identify instances of this being reported in UK

e. Virus-ransomware

What security arrangements do you have in place on your networks, and on laptops, computers and phones, to prevent virus or ransomware attacks?
Anti-Virus, Data Encryption, VPN, staff education and protect messaging. Unable to access certain domains using work computers. Unable to take work devices abroad without prior approval.

Would you say that these systems are state-of-the-art?
No

f. Bankruptcy-failure of operating company

Financial statements of proposed operating company for last five years.
https://www.westmidlands-pcc.gov.uk/transparency/about-the-office-of-the-west-midlands-police-and-crime-commissioner/annual-reports

Press reports on the company, including any recent changes of senior management.
Complete basic Google search

Due diligence enquiries into the company.

g. Highlighting of system failures

How prevalent would you say is dissatisfaction with your LEAs treatment of privacy and data security issues?
Low

European Commission | Horizon 2020 European Union funding for Research & Innovation

Project funded by H2020 Programme – Grant Agreement number: 786993

Are there any particular journalists who highlight such issues?

No

h. Lobbyists

How many lobbyist groups operate in your country on privacy and data-related issues?

Unknown

How well resourced and respected are they?

If possible, please provide links to their webpages etc.

i. Technological failures

How robust are your networks and computer systems?

Robust and well maintained

Have there been any failures in the last five years?

Unable to comment

Could these past failures be used by others to discredit your use of the system?

Unable to comment

5. Reputational attacks (by press etc?)

Are you aware of any groups that may seek to attack your use of the system?

No – likely that privacy activists may have views if it comes into the public domain

Is there any previous evidence of such attacks?

No

REPLY 3

QUESTIONNAIRE

Data and information to establish possible magnitude of incidental and residual risks

Please supply the following information and answer the following questions:

Incidental Risks – by Source and Category

1. Individuals
    a. Use for personal career advancement

Do you think the system will help officers to do their jobs better? YES
Will this be rewarded by promotion, recognition, salary increases or bonuses? On case by case basis, valid only for the aspect of recognition.

Disciplinary arrangements for officers, including any related to misuse of data YES
Details of enquiries/procedures into misuse of position by staff during the last ten years N/A
Guidance issued to staff about privacy and confidentiality, treatment of witnesses, suspects, arrested individuals YES

    b. Corruption + selling access to data

Do you think there are any such problems in your country? NO
How prevalent is this?
Reports from inquiries into police corruption during the last ten years http://www.astynomia.gr/index.php?option=ozo_content&perform=view&id=49&Itemid=40&lang=
(Annually report about corruption cases in Greek language)

Any ongoing investigations into corruption N/A

    c. Vendettas against groups or individuals

Press reports about police bias N/A
Which groups do you think may be targeted? By whom? N/A
Complaints data from groups or individuals N/A

    d. Deals with contacts in criminal-commercial organisations

Have there been allegations about relationships with criminal or commercial organisations? N/A
Did any of these involve exchange of sensitive information? N/A
Have there been any enquiries into such issues in your country in the last ten years? N/A

    e. Mistakes, incompetence, inattention

How difficult do you find it to recruit well-qualified staff?
The majority of the Hellenic Police personnel studies at the Police Academy which is considered as a university level institution. Apart from that, the Police Personnel is being trained through their carrier from national training programs and additionally from different organisations such as FRONTEX and CEPOL. Below is the link from the Hellenic Police website concerning the Hellenic Police Academy.

http://www.astynomia.gr/index.php?option=ozo_content&perform=view&id=61&Itemid=52&lang=&lang=EN

Details of internal and external training programmes with respect to use of data There are national and European training programs referring to the proper use of data, (e.g. HELENIC MINISTRY OF DEFENCE, HPID, FRONTEX, EUROPOL)
How much supervision do junior staff get when handling personal data? Considering that Hellenic Police is a Hierarchy Structured Organisation, the staff (not exclusively junior) is being supervised on a constant basis.
Details of all relevant disciplinary hearings in the last ten years N/A
How do officers log in to their computers at present? Hellenic Police has developed a domain type network where the authorized staff gets access with its personal account
What security systems do you use? Password? Facial recognition? Fingerprints? As mentioned above

f. Embedded practices, legacy systems

How do you currently investigate persons of interest? Using the information cycle (Info coming from internal and open sources, cross checks at databases, usage of technical means etc.)
Do you explore social media such as Facebook and Twitter? YES
How do you access such data? Through PC
Are the computers and laptops you use up-to-date with anti-virus and other security systems? YES

2. LEAs

a. Inadequate management

Are all the management positions in your organisation currently staffed? YES
Would you say that your management is efficient and organised? YES
Do all lower-level staff get adequate supervision? YES

b. Weak governance

Annual reports for the last five years.
http://www.seedd.gr//tabid/131/Default.aspx
Please give details of your governance structure, including lines of reporting. http://www.astynomia.gr/images/stories//2015/organogramma_en.png
Do you have a Board of Governors? Does it have a Charter, or a Code of Conduct? http://www.astynomia.gr/index.php?option=ozo_content&perform=view&id=35&Itemid=14&lang=EN
Have there been any enquiries into the management or governance of any LEAs in your country in the last ten years? N/A

c. Lack of accountability

When officers make mistakes in your organisation, what happens next? There are disciplinary measures according to Presidential Decree 120/2008
Are there any staff appeal processes? YES
Do you have any Whistleblower protections in place? Law 2713/1999 and Law 2928/2001 article 9 paragraphs 2-4.

d. Relationships with other agencies

Do you share data with any other government or non-government agencies? YES
If so, what procedures are in place to monitor their use of your data? In Hellenic Police all the data which are shared are protected according the National Security Regulation (EKA) and Hellenic Police Correspondence Regulation (Presidential Decree 75/1987) which are both in line with the EU Council security rules of classified Information. Also in Greece Hellenic Data Protection Authority (HDPA) is a

constitutionally consolidated independent Authority which mission is the protection of the personal data and the privacy of individuals in Greece, in accordance with the provisions of Law 2472/97 and 3471/2006.

http://www.dpa.gr/portal/page?_pageid=33,40911&_dad=portal&_schema=PORTAL

Are you concerned about the trustworthiness of any of the agencies with which you deal? NO

e. Inter-departmental rivalries

Who would you say are your main rivals within the security or governmental system? N/A
Do you have a friendly and professional relationship with them? N/A
Have there been instances in the last ten years where they have sought to undermine your authority or that of your organisation? N/A

3. Political

a. Electoral gerrymandering

Report of electoral commission into elections during the last ten years
Do you trust the politicians in your country to stick by the rules during elections?

Have there been recent instances of politicians misusing personal or other data during election times?

b. Vendettas against groups - eg Jews, migrants

Are there any political groups in your country who express hate or otherwise deride particular groups?
How powerful are such groups?
Has there been any recent evidence of these groups misusing data on individuals?

c. Discriminatory policies, bias

Reports of sex, race or other Commissions

Does your country have anti-discriminatory policies and procedures in addition to those at EU level? NO
Would you say that your current government's policies with respect to sex, race or religious discrimination are robust? YES

d. Damaging political opponents

Have there been any instances of the misuse of data by politicians to discredit opponents in the last ten years?
Are you aware of any press reports of such activities?

e. Finding scapegoats

Do you think that your government seeks to deflect blame for failed policies?
Can you provide a recent example? Did it involve an individual or a group?

4. External

a. Professional hackers

Have there been any instances of LEA systems that have been hacked in the last ten years?
Are you aware of any professional groups operating in your country?
Have there been any inquiries into the operations of such groups? If so, can we have their reports?

b. Foreign governments - eg China, Russia

Has there been any concern in the last five years about foreign governments seeking to access your data?
Are there any countries you are particularly concerned about?
What counter-measures do you have in place to prevent such attacks?

c. Blackmail of officials

Have there been any cases where officials have been found to face undue pressure from external groups?
Have there been any enquiries into such problems in the last ten years?

d. Dark Web

Do you think the Dark Web constitutes a threat to privacy and the security of data?
Have there been any examples of data being sold on the Dark Web. If so, can we have details?

e. Virus-ransomware

What security arrangements do you have in place on your networks, and on laptops, computers and phones, to prevent virus or ransomware attacks?
Would you say that these systems are state-of-the-art?

f. Bankruptcy-failure of operating company

Financial statements of proposed operating company for last five years.
Press reports on the company, including any recent changes of senior management.
Due diligence enquiries into the company

5. Reputational attacks (by press etc?)

g. Highlighting of system failures

Are you aware of any groups that may seek to attack your use of the system?
Is there any previous evidence of such attacks?
How prevalent would you say is dissatisfaction with your LEAs treatment of privacy and data security issues?
Are there any particular journalists who highlight such issues?

h. Lobbyists

How many lobbyist groups operate in your country on privacy and data-related issues?
How well resourced and respected are they?
If possible, please provide links to their webpages etc.

i. Technological failures

How robust are your networks and computer systems?
Have there been any failures in the last five years?
Could these past failures be used by others to discredit your use of the system?

Project funded by H2020 Programme – Grant Agreement number: 786993

REPLY 4

QUESTIONNAIRE

Data and information to establish possible magnitude of incidental and residual risks

Please supply the following information and answer the following questions:

Incidental Risks – by Source and Category

1. Individuals
    a. Use for personal career advancement

Do you think the system will help officers to do their jobs better?
Will this be rewarded by promotion, recognition, salary increases or bonuses?
Disciplinary arrangements for officers, including any related to misuse of data
Details of enquiries/procedures into misuse of position by staff during the last ten years
Guidance issued to staff about privacy and confidentiality, treatment of witnesses, suspects, arrested individuals

If the designed SPIRIT tool will fulfill its tasks, it will definitely be a great help and support in the investigative work of a policeman.
I sincerely doubt that the use of SPIRIT tool, effective in investigation will be appreciated by the police officer's promotion or salary increase. The case solution itself will be appreciated in the form of recognition. If the case was particularly difficult, perhaps in rare cases a policeman might receive a bonus in the form of a financial reward.
Every check of the data by the SPIRIT tool should be registered in the program. The person completing the enquiry should indicate the identification of the case for which he or she wishes to receive a response. The register of checks made may be used to verify and control whether individual inquiries were justified, necessary and related to a specific case. If not, then a policeman abusing software for other purposes will definitely exceed his rights and should take into account the legal consequences.
Any illegal checks in police data systems, registers and other databases discovered in the last 10 years have been subject to both disciplinary and investigative action. If an illegal check causes the violation of certain civil rights, privacy or other rights, it is a reason to initiate further proceedings.
All checks are subject to registration, continuous supervision and control. Cases of abuse and unjustified and unlawful checks are rare.
Staff guidelines for privacy and confidentiality, the treatment of witnesses, suspects and detainees are a everyday routine of the investigator work.
Respect for the right to privacy and confidentiality, the witnesses or suspects rights is the duty of every investigator.

    b. Corruption + selling access to data

Do you think there are any such problems in your country? How prevalent is this?
Reports from inquiries into police corruption during the last ten years

Any ongoing investigations into corruption

Unfortunately, corruption is still detected among police officers in Poland. Fortunately, the scale of this phenomenon is small and decreasing. This is mainly due to the very high involvement of the Police's Internal Affairs Bureau and the Central Anti-Corruption Bureau.
Although corruption in the Polish Police has been decreasing in recent years, it is more and more common mainly among young corrupted police officers.
A part of crime in the police is selling access to data and police checks.
However, the scale of taking away any secrets - data from police databases to e.g. detectives, other companies or sharing confidential knowledge with criminal groups - is disturbing. The charges covered only 38 police officers in 2018 (9 less than in 2017). This concerned mainly "intentional passing of information by corrupt officers", but also situations resulting from simple carelessness.

One 2018 year example: Police officer accepted 55 000 PLN bribe from a detective company for checking persons in police ICT databases. What is particularly interesting officer worked in the department dealing with combating corruption.

c. Vendettas against groups or individuals

Press reports about police bias
Which groups do you think may be targeted? By whom?
Complaints data from groups or individuals

The use of police data for revenge and reconciliation between criminal groups is unknown. It should be noted that cooperation between police officers and organised crime groups is a marginal phenomenon.

d. Deals with contacts in criminal-commercial organisations

Have there been allegations about relationships with criminal or commercial organisations?
Did any of these involve exchange of sensitive information?
Have there been any enquiries into such issues in your country in the last ten years?

See 1b

e. Mistakes, incompetence, inattention

How difficult do you find it to recruit well-qualified staff?
Details of internal and external training programmes with respect to use of data
How much supervision do junior staff get when handling personal data?
Details of all relevant disciplinary hearings in the last ten years
How do officers log in to their computers at present?
What security systems do you use? Password? Facial recognition? Fingerprints?

The selection of qualified workers, in particular in the area of specialist police work and ICT skills, is indeed problematic.
Depending on the position held and the tasks performed, police officers have different access to information and databases.
Each access is individual (login, password, access card, chip, access only from specific computers in selected locations).

Each login and check is registered and requires specifying the number of the case to which it relates. Each police officer is checked before accessing the police databases by the Internal Security Agency. Only after veryfications and trainings he/she get access to these databases. Access and checks are subject to constant monitoring.

f. Embedded practices, legacy systems

How do you currently investigate persons of interest?
Do you explore social media such as Facebook and Twitter?
How do you access such data?
Are the computers and laptops you use up-to-date with anti-virus and other security systems?

Conducting an investigation in Poland does not differ from practices in other European countries. We use all sources of information within OSINT.

Activities are carried out in a procedural form, as well as classified police activities. All of them are conducted in accordance with the needs of the investigation. Access takes place on the basis of official requests to Internet providers, as well as through operational activities.

2. LEAs

a. Inadequate management

Are all the management positions in your organisation currently staffed?
Would you say that your management is efficient and organised?
Do all lower-level staff get adequate supervision?

Most of the managerial positions are occupied. Vacancies are filled on an ongoing basis. Assessment of management effectiveness in the Police is not within the scope of our duties and is not the subject of our work.

b. Weak governance

Annual reports for the last five years.
Please give details of your governance structure, including lines of reporting.
Do you have a Board of Governors? Does it have a Charter, or a Code of Conduct?
Have there been any enquiries into the management or governance of any LEAs in your country in the last ten years?

not relevant

c. Lack of accountability

When officers make mistakes in your organisation, what happens next?
Are there any staff appeal processes?
Do you have any Whistleblower protections in place?

Any mistake or offence found to have been committed by a police officer shall be the subject of an investigation and disciplinary action. Where it is proved that the intention was intentionally committed, this shall be a criminal prosecution.
Clearly, appeal procedures are provided for in these proceedings.

We do not have an established Whistleblower institution in the police force.

d. Relationships with other agencies

Do you share data with any other government or non-government agencies?
If so, what procedures are in place to monitor their use of your data?

Are you concerned about the trustworthiness of any of the agencies with which you deal?

Of course, we make the data available to other security institutions. This is strictly provided for in specific regulations, only on official request and through specific secure channels of communication. Any inquiry from another institution must be legal and justified by the need to use it in a specific case.

e. Inter-departmental rivalries

Who would you say are your main rivals within the security or governmental system?
Do you have a friendly and professional relationship with them?
Have there been instances in the last ten years where they have sought to undermine your authority or that of your organisation?

It is not possible to say that such a competition exists. There have been no cases of undermining the authority of another service.

3. Political

a. Electoral gerrymandering

Report of electoral commission into elections during the last ten years
Do you trust the politicians in your country to stick by the rules during elections?
Have there been recent instances of politicians misusing personal or other data during election times?

We do not have any information to support such statements.

b. Vendettas against groups - eg Jews, migrants

Are there any political groups in your country who express hate or otherwise deride particular groups?
How powerful are such groups?
Has there been any recent evidence of these groups misusing data on individuals?

Yes, there are such extremist groups, extreme right-wing groups and anarchists. We have some information that members of these groups have illegally obtained personal data and used it against their opponents.

c. Discriminatory policies, bias

Reports of sex, race or other Commissions
Does your country have anti-discriminatory policies and procedures in addition to those at EU level?
Would you say that your current government's policies with respect to sex, race or religious discrimination are robust?

Yes, we have an anti-discrimination policy in every respect. It is in line with EU objectives.

d. Damaging political opponents

Have there been any instances of the misuse of data by politicians to discredit opponents in the last ten years?
Are you aware of any press reports of such activities?

There have been cases like this. They concerned different issues, e.g. sexual orientation, origin.

e. Finding scapegoats

Do you think that your government seeks to deflect blame for failed policies?
Can you provide a recent example? Did it involve an individual or a group?

Every government blames its opponents for the failed policy.

4. External

a. Professional hackers

Have there been any instances of LEA systems that have been hacked in the last ten years?
Are you aware of any professional groups operating in your country?
Have there been any inquiries into the operations of such groups? If so, can we have their reports?

There were no such situations.

b. Foreign governments - eg China, Russia

Has there been any concern in the last five years about foreign governments seeking to access your data?
Are there any countries you are particularly concerned about?
What counter-measures do you have in place to prevent such attacks?

Information about the activity of the online trolls or other persons who may be acting in different ways to the detriment of the state will appear. Some of them have links to other countries

c. Blackmail of officials

Have there been any cases where officials have been found to face undue pressure from external groups?
Have there been any enquiries into such problems in the last ten years?

There have been cases of officials being blackmailed by members of organised crime groups. Every known case was investigated.

d. Dark Web

Do you think the Dark Web constitutes a threat to privacy and the security of data?
Have there been any examples of data being sold on the Dark Web. If so, can we have details?

It is obvious that Dark Web is a huge threat, being a place of illegal transactions concerning, among others, personal data.
The database of customers of one of the big online shops was hacked, the perpetrator threatened to sell the customers' data also in Dark Web.

e. Virus-ransomware

What security arrangements do you have in place on your networks, and on laptops, computers and phones, to prevent virus or ransomware attacks?
Would you say that these systems are state-of-the-art?

We use all kinds of software security and antivirus software. In addition, we use hardware protection and the separation of the open Internet from the internal police network.

f. Bankruptcy-failure of operating company

Financial statements of proposed operating company for last five years.
Press reports on the company, including any recent changes of senior management.
Due diligence enquiries into the company.

Not relevant.

5. Reputational attacks (by press etc?)

a. Highlighting of system failures

Are you aware of any groups that may seek to attack your use of the system?
Is there any previous evidence of such attacks?
How prevalent would you say is dissatisfaction with your LEAs treatment of privacy and data security issues?
Are there any particular journalists who highlight such issues?

Issues related to privacy protection are the priority of LEA's activity in Poland. It should be stated that the society is satisfied with the protection of privacy assured by LEA's.

b. Lobbyists

How many lobbyist groups operate in your country on privacy and data-related issues?
How well resourced and respected are they?
If possible, please provide links to their webpages etc.

We don't have that kind of information.

c. Technological failures

How robust are your networks and computer systems?
Have there been any failures in the last five years?
Could these past failures be used by others to discredit your use of the system?
There were no failures that could in any way discredit the operation of the system.

Project funded by H2020 Programme – Grant Agreement number: 786993

9. References

Alonso Blas, D., 2010. "Ensuring effective data protection in the field of police and judicial activities: some considerations to achieve security, justice and freedom". In *ERA-Forum* Vol. 11 (2): 233-250.

Bertheau R.C., von Stackelberg O., Weckbach S., Kauczor HU., Schlett C.L. 2016. "Management of Incidental Findings in the German National Cohort". In: Weckbach S. (eds) I*ncidental Radiological Findings. Medical Radiology*. Cham: Springer, pp. 57-70.

Bigo, D., 2013. "The transnational field of computerised exchange of information in police matters and its European guilds". In Kauppi, N. and Madsen, M.R. (Eds.) *Transnational power elites: The new professionals of governance, law and security. In Transnational Power Elites*, London: Routledge, pp.155-182.

Bunnik, E.M., van Bodegom, L., Pinxten, W., De Beaufort, I.D., Vernooij, M.W., 2017. "Ethical framework for the detection, management and communication of incidental findings in imaging studies, building on an interview study of researchers' practices and perspectives". *BMC medical ethics*, *18* (1): 10. https://bmcmedethics.biomedcentral.com/articles/10.1186/s12910-017-0168-y

Casanovas, P., 2017. "Cyber warfare and organised crime. A regulatory model and meta-model for open source intelligence (OSINT)". In Taddeo, M. Glorioso, L. (eds). *Ethics and policies for cyber operations: a NATO Cooperative Cyber Defence Centre of Excellence initiative*, Cham: Springer, pp. 139-167.

Casanovas, P., Arraiza, J.I., Melero, F., González-Conejero, J., Molcho, G. and Cuadros, M., 2014. "Fighting Organized Crime Through Open Source Intelligence: Regulatory Strategies of the CAPER Project". In R. Hoekstra (ed.) *Legal Knowledge and Information Systems: JURIX 2014: The Twenty-Seventh Annual Conference*, vol. 271, Amsterdam: IOS Press. pp. 189-198.

Casanovas, P., Mendelson, D. and Poblet, M., 2017. "A Linked Democracy Approach for Regulating Public Health Data". *Health and Technology*, *7* (4): 519-537.

Custers, B., 2012. "Technology in policing: Experiences, obstacles and police needs". *Computer law & security review*, *28* (1): 62-68.

Custers, B., Vergouw, B., 2015. "Promising policing technologies: Experiences, obstacles and police needs regarding law enforcement technologies". *Computer Law & Security Review*, *31* (4): 518-526.

Damjanovicova, M., 2016. "Incidental Findings". In *Ethical Counselling and Medical Decision-Making in the Era of Personalised Medicine*. In Boniolo, S. Sanchini V (eds.), Cham: Springer Briefs, pp. 89-95.

De Hert, P., & Papakonstantinou, V. 2016. "The new police and criminal justice data protection directive: A first analysis". *New journal of European criminal law*, 7 (1): 7-19.

Elmqvist, J., Nadjm-Tehrani, S., 2007. "Safety-oriented design of component assemblies using safety interfaces". In Third International Workshop on Formal Aspects of Component Software (FACS'06) , pages 1–15, Prague, Czech Republic, September. *Electronic Notes in Theoretical Computer Science*, *182*, pp.57-72.

Elmqvist, J., Nadjm-Tehrani, S., 2008. Formal support for quantitative analysis of residual risks in safety-critical systems. In *High Assurance Systems Engineering Symposium, 2008. HASE 2008. 11th IEEE* IEEE, pp. 154-164.

Erdmann, P., 2016. "Incidental Findings–Ethical Aspects". In Weckbach, S. (ed.), *Incidental Radiological Findings* Cham: Springer, pp. 9-24.

U Council of Europe's Convention on Cybercrime (ETS No 185). 23/11/2001. http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf

EU Regulation (EU) 2016/679 of the European Parliament and of the Council 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, and repealing Directive 95/46/EC (General Data Protection Regulation) https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

EU Directive (EU) 2016/680 of the European Parliament and of the Council 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, and repealing Council Framework Decision 2008/977/JHA. http://data.europa.eu/eli/dir/2016/680/oj

EU Committee of Ministers. *Recommendation CM/Rec (2017) 6 of the Committee of Ministers to member States on "special investigation techniques" in relation to serious crimes including acts of terrorism* (Adopted by the Committee of Ministers on 5 July 2017 at the 1291 st meeting of the Ministers' Deputies. https://rm.coe.int/1680730408

EU Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. *Practical guide on the use of personal data in the police sector*. Strasbourg, 15 February 2018 T-PD (2018)01. https://rm.coe.int/t-pd-201-01-practical-guide-on-the-use-of-personal-data-in-the-police-/16807927d5

Floyd, H.L., Floyd, A.H., 2017. "Bringing attention to residual risk: Psychology of Warnings, Administrative Controls and PPE". In *Electrical Safety Workshop (ESW), 2017 IEEE IAS*. IEEE, pp. 1-5.

Gheorghe, A.V., Mock, R., 1999. "Established Methods in Risk Engineering". *In Gheroge and Moch (eds.), Risk Engineering. Bridging Risk Analysis with Stakeholders Values.* Dordrecht: Springer, pp. 61-120.

Grassi, P. et al. 2017. *Digital Identity Guidelines. Authentication and Lifecycle Management*. NIST Special Publication, USA, 800-63B.

Hanna, T.N., Shekhani, H., Zygmont, M.E., Kerchberger, J.M., Johnson, J.O., 2016. "Incidental findings in emergency imaging: frequency, recommendations, and compliance with consensus guidelines". *Emergency radiology*, *23*(2): 169-174.

Havinga, H.N.J., Sessink, O.D.T., 2014. "Risk Reduction Overview". In *International Conference on Availability, Reliability, and Security* , in S. Teufel et al. (Eds.), CD-ARES 2014, LNCS 8708, Springer: Cham, pp. 239-249.

ITU-T, Baseline identity management terms and definitions Recommendation ITU-T X.1252, Annex A, p.8, http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=X.1252

Jasserand, C., 2018. "Law enforcement access to personal data originally collected by private parties: Missing data subjects' safeguards in directive 2016/680?". *Computer Law & Security Review*, *34*(1): 154-165.

Johnsen, A., Crnkovic, G.D., Lundqvist, K., Hänninen, K., Pettersson, P., 2017. "Risk-based Decision-making Fallacies: Why Present Functional Safety Standards Are Not Enough". In *2017 IEEE International Conference on Software Architecture Workshops (ICSAW)*, April 2017, pp. 153-160.

Kappes, M.S., Keiler, M., von Elverfeldt, K. and Glade, T., 2012. "Challenges of analyzing multi-hazard risk: a review". *Natural hazards*, *64* (2): 1925-1958.

Harmon, R.A. 2012. "The Problem of Policing", 110 *Michigan Law Review,* pp. 761-785.

Ladenburger, C., 2008. "Police and criminal law in the Treaty of Lisbon: A new dimension for the Community method". *European constitutional law review*, *4* (1): 20-40.

Lawrenz, F., Sobotka, S. 2008. "Empirical analysis of current approaches to incidental findings." *The Journal of Law, Medecine and Ethics* (2008), pp. 249-255.

Leveson, N., 2011. *Engineering a safer world: Systems thinking applied to safety*. Cambridge, MA: MIT press.

Leveson, N. 2013. Engineering a Safer World. Tokyo Seminar 20140121. Presentation. https://slideplayer.com/slide/4659106/15/images/1/Engineering+a+Safer+World.jpg

Malatras, A., Sanchez, I., Beslay, L., Coisel, I., Vakalis, I., D'Acquisto, G., Sanchez, M.G., Grall, M., Hansen, M., Zorkadis, V., 2017. "Pan-European personal data breaches: Mapping of current practices and recommendations to facilitate cooperation among Data Protection Authorities". *Computer Law & Security Review*, *33* (4): 458-469.

Marquenie, T. 2017. "The Police and Criminal justice Authorities Directive: Data protection standards and impact on the legal framework". *Computer Law & Security Review*, *33* (3): 324-340.

NIST Information Technology Laboratory. Computer Security Resource Center. *Risk Management*. Updated 11 September 2018. https://csrc.nist.gov/Projects/Risk-Management/Risk-Management-Framework-(RMF)-Overview

Schermer, B.W., Custers, B. , van der Hof, S., 2014. The crisis of consent: How stronger legal protection may lead to weaker consent in data protection. *Ethics and Information Technology*, *16* (2): 171-182.

Schmücker, R., 2016. Incidental Findings: Definition of the Concept. In: Weckbach S. (eds) I*ncidental Radiological Findings. Medical Radiology*. Cham: Springer, pp. 3-7.

Stoughton, S.W., 2013. "Policing Facts". *Tulane Law Review*, *88*, pp. 847-898.

Stoughton, S. W. 2014. "The Incidental Regulation of Policing." *Minnesota Law Review* 98, pp. 2179-2235.

Stoughton, S.W., 2016. "Principled policing: Warrior cops and guardian officers". *Wake Forest L. Rev.*, *51*, pp.611-676.

Torra, V. 2017. *Data Privacy: Foundations, New Developments and the Big Data Challenge*. Cham: Springer International Publishing.

Tosoni, L., 2018. Rethinking Privacy in the Council of Europe's Convention on Cybercrime. *Computer Law & Security Review* (forthcoming). https://www.sciencedirect.com/science/article/pii/S0267364918303091

US Government: Presidential Commission for the Study of Bioethical Issues (Bioethics Commission) in *Anticipate and Communicate: Ethical Management of Incidental and Secondary Findings in the Clinical, Research, and Direct-to-Consumer Contexts.* Washington, D.C. December 2013.

US Government: Presidential Commission for the Study of Bioethical Issues (Bioethics Commission), *For Researchers: Incidental and Secondary Findings,* last update 30/10/2016.

UK Government: *Identity Proofings and Verification of an Individual*. https://www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual

Viberg, J., Hansson, M.G., Langenskiöld, S. and Segerdahl, P., 2014. "Incidental findings: the time is not yet ripe for a policy for biobanks". *European Journal of Human Genetics*, *22* (4), p.437.

Wilson, J.Q., 1978. *Varieties of Police Behavior: The Management of Law and Order in Eight Communities, With a New Preface by the Author*. Harvard University Press.

Wolf, S.M, Lawrenz F.P, Nelson C.A, et al. 2008. "Managing Incidental Findings in Human Subjects Research: Analysis and Recommendations". *J Law, Med Ethics*. 36 (2): 219–248. doi:10.1111/j.1748-720X.2008.00266.x.

Young W., Leveson. N. 2013. "Systems thinking for safety and security". In Proceedings of the 29th Annual Computer Security Applications Conference (ACSAC '13). ACM, New York, NY, USA, 1-8.