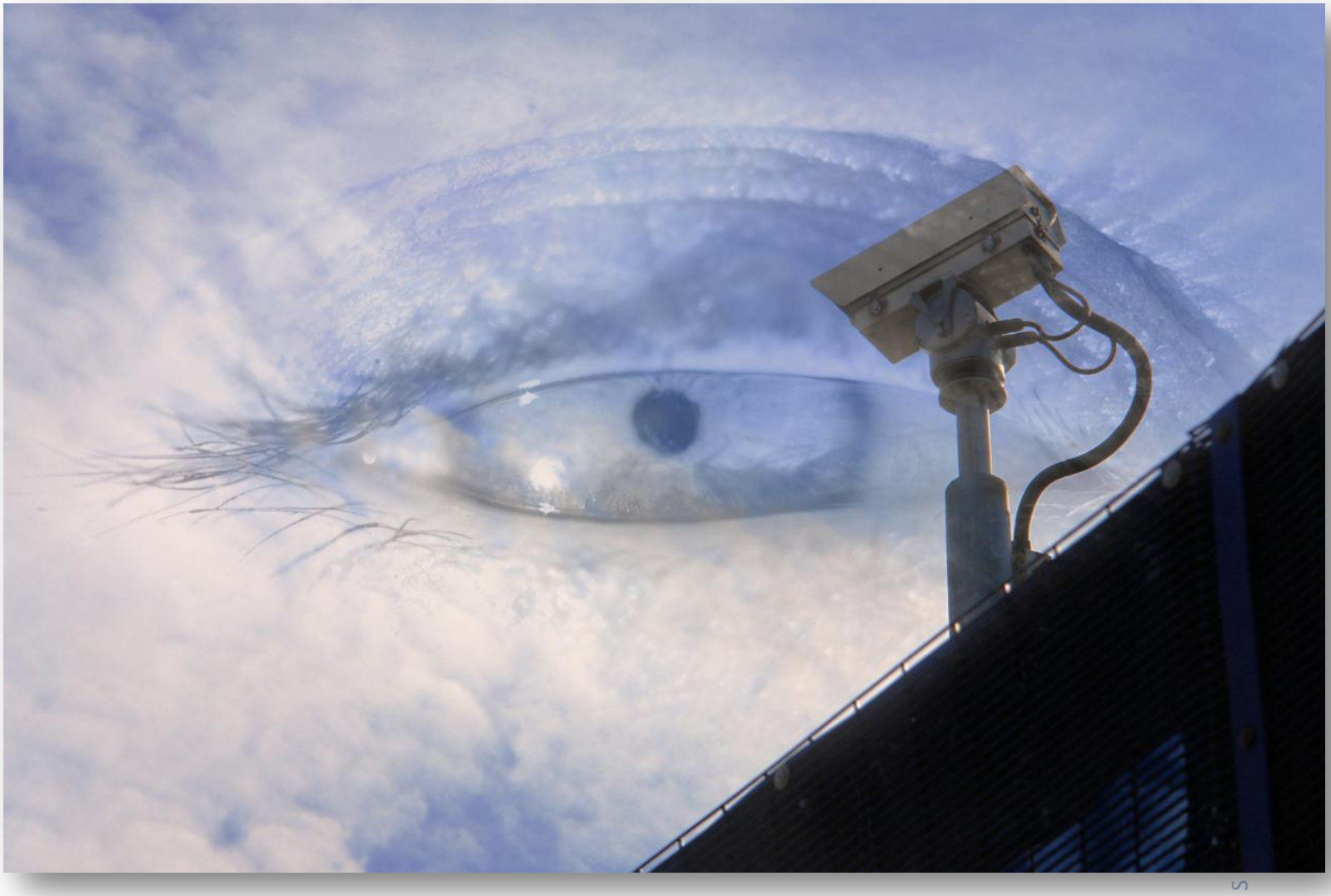


Privacy Impact Assessment (PIA) Guidelines for the Introduction of new Police Powers

Information Commissioner
of the Republic of Slovenia

INFORMATION COMMISSIONER GUIDELINESS

Scope	The main purpose of these guidelines is to provide a tool that law enforcement policy makers can use when introducing new police powers, particularly those entailing the use of technical measures. This tool will aid in conducting of a thorough privacy impact analysis (PIA), help in assessing the necessity, adequacy, effectiveness and proportionality of the new measures, allow for due public debate on the subject, and assist in providing adequate safeguards against serious infractions of fundamental constitutional rights.
Target audience(s)	Law enforcement, Office of the Attorney General, Ministry of Justice, general public
Status	Public
Version	1.0 (English Translation)
Date of publication	14 January 2014 (translation April 2014)
Author(s)	Information Commissioner of the Republic of Slovenia
Keywords	guidelines, police powers, technical measures, privacy, data protection, privacy impact analysis, proportionality, test of proportionality

Table of contents

About the guidelines of the Information Commissioner of the Republic of Slovenia

The Information Commissioner of the Republic of Slovenia provides detailed guidelines on various subjects in order to provide clear, detailed and easy to use answers to frequently asked questions regarding data protection and privacy. Using the guidelines, data controllers can better understand the requirements as laid in the Personal Data Protection Act of Slovenia (ZVOP-1).

The legal basis for these guidelines is provided by Article 49 ZVOP-1, which, inter alia, allows the Commissioner to issue non-binding opinions and recommendations on various data protection related topics, and to publish them on its website.

See also our:

- http://www.ip-rs.si/varstvo-osebnih-podatkov/iskalnik-po-odlocbah-in-mnenjih/smernice/ (guidelines);
- http://www.ip-rs.si/varstvo-osebnih-podatkov/iskalnik-po-odlocbah-in-mnenjih/ (decisions and opinions);
- http://www.ip-rs.si/publikacije/prirocniki/ (instruction booklets).

Abstract

The following Privacy Impact Assessment (PIA) Guidelines for the Introduction of New Police Powers (the Guidelines) provide a comprehensive framework for judicious, well-thought-out and legitimate introduction of new police powers, with particular focus on those with a strong technological aspect. The Criminal Procedure Act of Slovenia (the ZKP) has had its fair share of amendments over the last 20 years (with amendment #13 on the way), and has thus had many new police powers added. Unfortunately, not all of those proposals were accompanied by an adequate and detailed memorandum clearly laying out the necessity, suitability, effectiveness, and proportionality of the new measures. All too often, public debate of the new measures was limited, if done at all. Consequentially, usage of new powers has been riddled with difficulties, often subjected to exclusion of evidence before the courts of law, and sometimes met with outright dissent by both the general as well as professional public.

To help with these issues, the guidelines lay out a comprehensive framework for conducting a pre-emptive Privacy Impact Assessment (PIA) of new legislative proposals dealing with police powers[1]. The guidelines are divided into four phases, as follows. In the **first phase**, an initial assessment is to be carried out, detailing the needs for the new police power, and clearly explaining the benefits of the said power. If the new power is of a technical nature, a detailed description of its capabilities is particularly paramount. Then, in the **second phase**, the various risks regarding the use of the power are to be identified, with special focus on risks regarding the impact the proposed measure will have on constitutional rights of privacy and protection of personal data, and risks regarding the overall effectiveness of the measure. Also, a comparative legal study detailing the use of the measure in other countries is to be performed, taking into account not just what can be done, but also, how it should be done and which pitfalls are to be avoided. In the **third phase**, safeguards must be introduced to deal with all the identified risks (i.e. the minimal standard of proof, requirements for court authorization, minimization procedures, etc.). Finally, in the **fourth and final phase**, all the information gathered in the previous phases is used to conduct a thorough test of proportionality. Should the measure not pass this test, for instance because it may be found as not suitable enough, as ineffective, or simply because the measure would inflict disproportionate harm to the fundamental constitutional rights of suspects and third parties, such a measure will have to be reconsidered before it can be tabled for inclusion into the criminal procedure law. For only if these steps are followed can we be sure that the use of the measure will be legitimate, effective, and accepted by both courts and the general public alike.

The overall procedure for conducting of said PIA analysis is as follows:

1. The initiating party (the party proposing the new measure, usually the Slovenian Police / Ministry of the interior) is to conduct a Privacy Impact Assessment of the measure using these guidelines, and then submit a written report to the Information Commissioner for comment;
2. The Information Commissioner reviews the report and submits comments as needed;
3. The initiating party addresses the comments and amends the analysis report if so needed;
4. The initiating party drafts the legislative proposal regarding the new police powers, and submits it, along the PIA report, to the ministry responsible for the Criminal Procedure Law (the Ministry of Justice), along with the remark detailing whether the text respects the comments from Information Commissioner or not;
5. The bill proposal enters the standard legislative process.

[1] Note: the Guidelines are meant to be used primarily by the Slovenian Police, but may lend themselves useful to other entities involved with criminal law, i.e. the Ministry of Justice, the Attorney General, and the Courts.

Introduction

When introducing new police powers, one must observe that the fundamental purpose of criminal law is the limitation of state powers against individuals, in particular the powers of police as the most significant agent of the state in criminal and security matters. Ever since the French revolution, the main safeguards against the arbitrary action of police forces have always been the now internationally-accepted human rights, such as equality before law, prohibition of torture, the protection of personal liberties, the presumption of innocence, safeguarding of human dignity and privacy, and the like. All these rights are more concretely defined in criminal procedure law. Thus, given that the level of rights afforded to suspects in police procedures serves as an important benchmark of the state of democracy in a particular country, it is absolutely paramount that all (new) police powers are proportionate to the degree of harm they inflict upon those rights, and that all laws that embody such powers are well-defined, concrete, and predictable[2].

The Information Commissioner has in recent years seen several cases where new legislative proposals were not always accompanied by adequate analysis and justification (particularly regarding recent amendments to the Criminal Procedure and Electronic Communications acts), and in some cases public discourse regarding the same proposals was limited if not nonexistent.

On the need for a comprehensive framework for introducing new police powers

In recent years, the process of introducing new police powers is Slovenia has been a cause for quite some concern. We have witnessed a near symptomatic series of questionable amendments to the Criminal Procedure Act, prepared without using a comprehensive framework that would allow for:

- conducting of a privacy impact assessments;
- justification of the necessity, adequacy, effectiveness, and proportionality of the new measures;
- analysis of the risks involved with these new measures;
- thoroughly addressing those risks, and
- defining the criteria for subsequent analysis of the impact of the adopted measures (the follow-up Regulatory Impact Analysis).

In general, the process of introducing new police powers would start by simply **noting the availability of a specific new technology** in the law enforcement market (i.e. IMSI catchers, drones, police trojan horse software, bulk metadata collection and analysis software), or by **observation that current investigations are no longer as successful as they should be**, seeing that criminals have started using certain new, technologically sophisticated tools that have proven to be partially or fully impervious to existing law enforcement techniques (e.g. use and regular swapping of pre-paid SIM cards or switching to encrypted VoIP services). This realization was then followed up by a nigh-immediate drafting of new amendments that would, as is argued, allow the police to somehow circumvent these problems. **No prior privacy impact analysis (PIA) was performed** and no subsequent impact analysis (RIA)

[2] Logar, Jure: On the sensitive issue of introducing new police powers. Ljubljana: GV Založba. Pravna praksa št. 5/2013 (in Slovene)

envisioned. **The accompanying memoranda** to the bill that should have explained and justified the new provisions were **found to be lacking**, and in some cases questionable[3] if not outright misleading[4].

Perhaps it was also because of those shortcomings that most of these proposals were rejected early in the formal inter-ministerial coordination process; however, some did make it into the legislative procedure before the national parliament. The most recent amendments to the Criminal Procedure Act (ZKP) and the Electronic Communications Act (ZEKom-1) even managed to secure parliamentary vote, becoming law. Some measures in those bills are questionable not just in regard to their proportionality, but were also not adequately explained, making it quite difficult for the Information Commissioner and the public to decipher what exactly is it they mean. This has greatly hindered the discourse regarding the measures within the general and competent public.

The use of these new measures thus raises grave questions regarding their impact on certain fundamental constitutional rights such as those of privacy, protection of personal data, freedom of speech, and freedom of assembly. One must recall that, according to the long-standing constitutional principles, breaches of fundamental rights are only allowed if deemed proportionate, which in the jurisprudence of the Constitutional Court of Slovenia means passing the standard three-step proportionality test[5]:

1. The breach must be **necessary**[6];
2. The breach must be **adequate**, and thus **effective** in reaching the desired, constitutionally-valid goal;
3. The breach must be **proportional in the narrower sense**; meaning that the benefits of the breach significantly outweigh its negative side effects for the suspects' or others' constitutional rights.

The crux of the proportionality test is indeed in weighing the latter two aspects, thus searching for the fine balance between ensuring the safety of others and violating the privacy of the (would be) suspect. Both tips of the scale should - at the very least - be identified and well described. The explanatory memorandum to the bill should, in example, include a justification as to why obtaining cell tower dumps (a recent proposal) is indeed necessary, and why metadata obtained for individual mobile phones is no longer sufficient (or in other words: why the same goal may not be achieved via lesser means). The proposal must also be proportional in the narrower sense, elaborating why breaching the privacy of perhaps several hundred people who just happened to have used that specific cell tower is really justified to solve specific (and if so - which) crimes.

Furthermore, the effectiveness of the proposal must also be justified. Given that it is not unheard of for organized crime to use disposable phones (or simply leave them at home during the commission of crimes), would cell tower dumps truly be effective at solving such crimes? Or would we end up collecting data only on completely innocent people?

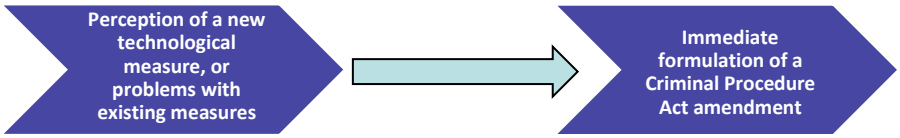
[3] Upon ratifying the EU Data Protection Directive in 2006, the government chose the longest possible retention period of two years (24 months), arguing that the extra storage capacity required would pose no significant cost for the operators, while providing an important benefit towards prosecution of crimes.
[4] In late 2012, while reforming the Electronic Communications Act, the police and intelligence service of Slovenia tried to sneak in an amendment that would have granted them access to retained traffic data without the use of an appropriate warrant.
[5] Judgment of the Constitutional Court of the Republic of Slovenia, case U-I-137/93 from June the 2nd, 1994, see http://odlocitve.us-rs.si/usrs/us-odl.nsf/o/A22D391E8E3171DDC1257BF0003AA18F (available in Slovenian).
[6] Meaning that the same goal cannot be attained using lesser (less invasive) means.

It is noteworthy that newer, technologically more advanced police gadgets only offer more possibility for collecting the subjects' data, and thus interfering with their constitutional rights. The more recent bill proposals, however, fail to take that into account, and never truly address the proportionality of the proposed measures. The only criterion for adoptions seems to be increasing the effectiveness of the police, particularly in alleviating any difficulties with obtaining suspect data that might pop up. For instance, the police may complain, that "certain" (but not all) mobile providers refuse to provide cell tower dump data, and thus an explicit provision for this simply must be added to the Criminal Procedure Act. The privacy impact analysis, however, is simply overlooked. Consequently, the proposed provisions will tend to raise serious doubts regarding their proportionality, and will be poorly received by the general public.

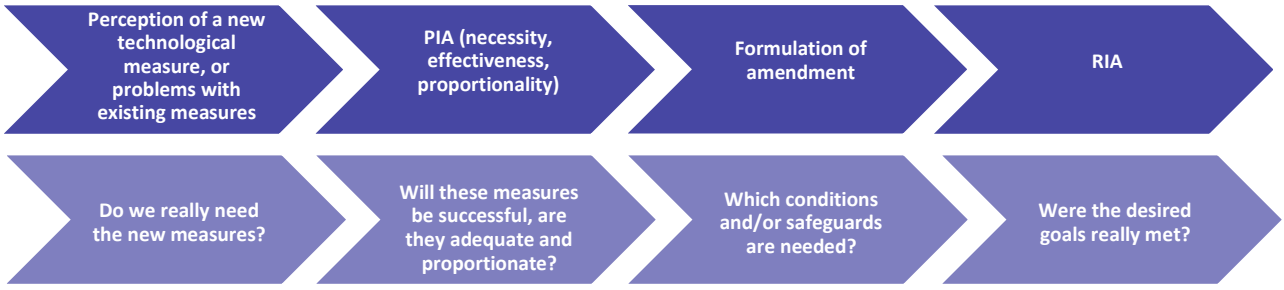
There are many far-reaching consequences of not conducting a proper PIA:

- Public discourse of the bill is impossible, or at best limited[7];
- Revocation of ill-enacted police measures is not possible, or is slow at best (usually through judgments of the Constitutional court, several years down the line);
- The privacy of citizens continues to suffer;
- The inefficiencies caused by the lack of a proper PIA and subsequent RIA analysis are borne by everybody[8], both by loss of the right of privacy and the inability to solve crime even with these new measures.

We must thus move away from the current state…



.. Into this state:



For the reasons as outlined above, The Information Commissioner of the Republic of Slovenia has prepared guidelines for introduction and amending new police powers, particularly those related to certain technologies which use may entail substantial breach of privacy or collection of personal data on a massive scale (technologies like drones, biometric face recognition, automated license plate recognition, retention of traffic metadata, etc.). The main goal of these guidelines is to outline an

[7] The quality of discussion will tend to be limited when in regard to more general terms such as »technical measures«, as opposed to, say, electro shockers, which were already met with strong and flavorful discussion in the past.
[8] A 2008 report by the Max Planck institute shows that telecommunications data retention hasn't led to a discernible increase in the percentage of solved crimes see http://www.vorratsdatenspeicherung.de/images/mpi-gutachten.pdf . The costs of such an operation still have to be borne by the subscribers, though.

appropriate methodological approach for adopting invasive technologies and new police powers - one that includes a timely and comprehensive identification and management of the specific risks involved in using those technologies or powers, and conducts the required analysis of the necessity, suitability, effectiveness, and proportionality of the new measures with regard to personal privacy (a Privacy Impact Assessment - PIA), and possibly also includes a regular after-the-fact analysis of the measures (a Regulatory Impact Analysis - RIA). The end goal is effective and legal functioning of the police, producing credible and admissible evidence in court, and consequently yielding a higher crime clearance rates - all while taking account of the balance between protecting the public and the human rights afforded to suspects, and of course non-suspects (third parties with the misfortune of getting caught up into these new measures by way of collated damage).

As already stated, the guidelines deal mainly with police measures that include mass collection of private data, particularly using modern information-communication technologies. These include measures already in use by the police as well as those likely to be put in use in the near future, for instance:

- Unmanned aerial vehicles (drones);
- Biometric facial recognition;
- Automatic license plate recognition;
- Mandatory retention of electronic communications data;
- Source-based lawful interception of encrypted voice traffic (trojans, rootkits, spyware);
- False mobile towers allowing for identification, tracking and surveillance of mobile phones (IMSI catchers, stingrays);
- Intelligent video surveillance;
- Security robots;
- Thermo vision, infrared and other advanced surveillance cameras.

As a side note, it is important to note that a prior (ex ante) privacy impact analysis is but one part of a wider process of analyzing the impact of legislation[9]. A variety of other prior and posterior (after the fact) methods exist and should be employed, as needed, in order to systematically address the various effects of legislation[10]. The Court of Audit of the Republic of Slovenia recently released a report titled "Do Slovenian institutions properly assess the impact of proposed legislation on society?"[11], in which the Court suggested that such checking should become standard practice, so to enable the country to better respond to social changes.

[9] Resolution on Legislative Regulation, see http://zakonodaja.gov.si/rpsi/r06/predpis_ZAKO5516.html (in Slovene)
[10] Article 6 of the Resolution sets the rationale for reviewing the impact of legislation: improving the quality of new legislation, simplification of the legislative process, and checking for attainment of legislative goals. Well-planned and systematically executed reviews, especially of key pieces of economic, social and environmental legislation, provide the legislator and the other involved parties with critical information needed in their decision making process.
[11] The two part report is available on the website of The Court of Audit, see http://www.rs-rs.si/rsrs/rsrs.nsf/I/K7AAECFAFA8DFD535C1257A62001C1180 (in Slovene).

What benefits can the police expect by conducting a Privacy Impact Analysis?

1. Any further proposals for introducing new police powers will be accompanied with a comprehensive analysis clearly laying out the necessity, adequacy, effectiveness, and proportionality of the new measures, thus giving them a much needed sense of legitimacy;
2. The proposals are less likely to be met with negative comments by the general and professional public, as was the case with some recent proposals;
3. By producing hard evidence and reasoning for the measure, court orders should be easier to obtain, and the gathered evidence is less likely to be the subject to exclusion, thus improving crime clearance rates.

Also, additional benefits for the society as a whole are:

1. Better transparency in adopting new measures, more public discourse;
2. Higher legitimacy and grounds for conducting regulatory impact analyses (RIAs) later on;
3. Better equilibrium and proportionality between new police powers and respective constitutional rights;

A methodological approach to analyzing the impact of police powers

What is a privacy impact assessment (PIA)?

A privacy impact assessment (PIA) is a tool for identification, analysis and mitigation of various privacy-related risks involved in a new project, system or use of technology, in particular risks regarding mass collection and processing of personal data and risks regarding serious invasions of privacy. PIAs are traditionally done in jurisdictions that place more legal emphasis on wider protection of privacy than on protection of personal data. They are a common (and sometimes mandatory) tool in Canada, Australia and the United States of America, but have begun picking up ground in the European legal space, where, traditionally, more emphasis is put on protection of personal data. They are well used in both the public and the private sector.

The crux of a well-executed PIA revolves around a systematic and thorough identification of privacy-related risks, thus allowing effective mitigation of said risks. PIAs follow the so-called "privacy by design principle", and go a long way in preventing "function creeps", that is use of already collected data for nefarious purposes not originally envisioned.

A PIA may be carried out internally or externally[12]; in both cases, the Information Commissioner can be brought in to provide advice and counsel. The Information Commissioner of the Republic of Slovenia

[12] Or by a combination of both methods (so-called “mixed” PIAs)

regularly works with stakeholders, both privately in meetings and by issuing written opinions, many of which are later published on our website. The Information Commissioner also issues written opinions on all new bill proposals that may influence privacy and data protection, and we are quite happy to see many of those opinions get implemented in practice.

The guidelines are focused on conducting an internal PIA, which is then to be submitted to the Information Commissioner for review and comments.

The basic principles of a Privacy Impact Assessment

The basic principles of a PIA directly reflect those of data protection in general:

Legality

The principle of legality requires the rules governing data protection to be clear, ascertainable and non-retrospective. Under the Constitution of the Republic of Slovenia (Article 38), the collection, processing, designated use, supervision and protection of the confidentiality of personal data must be in line with the law. Personal Data Protection Act (ZVOP-1) particularly stresses that in the public sector, processing of data is allowed only if explicitly allowed by law, in which case the data that is to be processed must also be particularly described. Processing of data on the basis of the subjects consent, or under the Article 7(f) of the Data Protection Directive, is generally viewed as insufficient in the public sector, and in particular in terms of police powers.

The governing law (i.e. the Criminal Procedure Act - ZKP, The Police Tasks and Powers Act - ZNPPol, the Electronic Communications Act – ZEKom-1, the Inspection Act - ZIN, the Gaming Act - ZIS) must thus provide explicit provisions allowing for processing of personal data by the respective public authorities, unequivocally detailing the data to be processed, and the purpose for which it is processed. These provisions must be as precise and clear as possible (lex certa), so that they can be understood and used fully and properly by those tasked with administering them. Uncertain provisions tend to lead to different interpretations, which can be particularly dangerous in the realm of criminal law. The principle of legality thus guarantees legal certainty, predictability and equality, as required by the Resolution on Legislative Regulation adopted by the Parliament of Slovenia.

Greater legal certainty also benefits individuals whose data is to be collected and processed, as well as large intermediaries such as ISPs and information service providers that tend to process lots of user data and are thus frequently subjected to law enforcement subpoenas for turning over of said data. As noted in a study published by the Information Commissioner last December, the Slovenian police would frequently demand data from various information society service providers simply on the basis of Article 148(1) of the Criminal Procedure Act, which provides them simply with a general obligation to investigate felonies, and not with a concrete legal basis for requiring (forcing) third parties to disclose data. The Information Commissioner argued that, if the latter were indeed the case, there would indeed be no need for the latter articles detailing their various investigative powers. Further, the Information Commissioner identified that several police powers were severely "under regulated", i.e. providing the police with the power to use unspecified "technical measures" (Article 113 of the new Police Tasks and Powers Act") or devices and software described simply as "decoders" or "measures that allow for determining the suspect's mobile phone number" (a recent Criminal Procedure Act

amendment proposal). It would be extremely difficult for courts to properly weigh-in on issuing warrants for using such "technical measures", and then to later, at trial, to prove that the evidence thus obtained was indeed legal. In fact, the Slovenian constitutional court has in several cases found the articles on covert investigative powers to be unconstitutional due to their lack of legality.

Fairness and Transparency

The processing of personal data must be fair and transparent to the individuals concerned. In particular, the purposes for which data is processed must be explicit and must be determined at the time of collection of the data; and further purposes of processing must not be incompatible with the purposes as they were originally specified. Whenever data is transferred or disclosed to third parties, especially to a law enforcement agency, a proper audit trail must be kept. Public sector requests for data must be based an appropriate provisions of law explicitly granting that right to the public agency, while private sector requests are possible only if the individual whose personal data is to be transferred gave his or her consent.

Proportionality

In the context of data protection, proportionality will generally mean that only personal data that is truly required for a specific purpose, may be collected and then processed. Thus if a particular item of personal data is not required for that specific purpose, it must not be collected much less processed or transferred to third parties. Blanket data collection is not to be tolerated, much less under the all too common guise that it is only the processing of that data which interferes with a person's rights of privacy and data protection (and that just collection is thus somehow justified). Furthermore, when less sensitive data will suffice, only that data may be collected (for instance, a person's full name will generally suffice, thus voiding the need to collect SSNs or passport numbers). Finally, once the data has served its intended purpose, and is thus not needed any more for that particular purpose, it must be deleted or appropriately anonymised.

Common examples of violations of the proportionality principle:

1. Simultaneous collection of multiple unique identifiers (VAT number, personal identification number, SSN, passport number, etc.);
2. Blanket data collection ("fishing expedition");
3. Collection of data for a yet unspecified purpose ("just in case");
4. Collection of data due to legacy requirements ("Our system requires this and this identification number.", "These are the forms we use.", etc.);
5. The general tendency of the police to collect and process as much data as possible, if only for use in possible future investigations[13].

Accuracy and timeliness

Personal data must be accurate and timely, meaning it must not be wrong, incomplete, or out-of-date. Processing of inaccurate and/or out-of-date personal data can have disastrous consequences. The

[13] For instance, the tendency to fingerprint, photograph and swab every suspect brought to police headquarters, regardless of the fact whether those samples are actually needed in that specific case.

Information Commissioner has noted cases of the police arresting or investigating completely innocent people on the basis of a misspelled SSN number, or local authorities issuing fines to owners of license plates that were reported stolen long ago and belonged to a completely different vehicle. In most of these cases, the wronged individual can be subjected to steep punishment, and will have to go to utmost difficulties in order to prove his or her innocence. No-flight and other similar "blacklists" pose particular danger to personal rights if they are not updated in an accurate and timely manner.

Retention periods

Personal data may be stored for longer periods than those necessary for the purposes for which the data were collected or for which they are further processed. Upon attainment of said purposes, or upon expiration of said retention terms, personal data may no longer be kept in a form that allows for the identification of data subjects, and must thus be deleted and/or appropriately anonymized, in line with applicable safeguards for personal data stored for longer periods for historical, statistical or scientific use.

One of the core tasks of a PIA assessment is determining the maximum term (time period) for which personal data is to be stored. In doing that, one must ask themselves what is the absolute minimum period that still allows for attaining the desired purpose is, and then keeping the data only that long. For instance, a recent study[14] by the EU Commissions shows that 70% of requests for traffic data relate to event no older than 3 months, and that a full 88% percent relate to those no older than 6 months. In lights of this, proportionality of longer data retention terms (14 months, 5 years, etc.) may be brought under question.

Data security

Appropriate technical and organizational measures must be taken to ensure the confidentiality, integrity and availability of personal data in order to prevent inadvertent or malicious loss, theft, manipulation and unjustified processing of personal data. Use and transfer of personal data should be logged and monitored, when appropriate, to allow for detection of such incidents.

Respect for fundamental rights of data subjects

This core principle of data protection relates to the person whose data is to be collected and processed. The data subject is to be informed that processing or transfer of his or her personal data is taking place, to consult the data, to request corrections and even to object to processing in certain circumstances. In particular, the subject should (eventually) be able to determine whether and why his or her personal data were passed to police authorities, allowing of course for reasonable delays to those rights in the interest of pending investigations.

[14] http://www.statewatch.org/news/2011/apr/eu-com-data-retention-report-225-11.pdf

PIA models

The Information Commissioner has consulted various approaches to PIA methodologies and ascertains that multiple PIA models exist that are used in different scenarios[15].

1. All-encompassing or full-scale PIAs;
2. Small-scale PIAs;
3. Privacy requirements checklists;
4. Data protection requirements checklists.

In the context of these guidelines, we recommend the use of a **small-scale PIA in conjunction with a checklist**[16]. We feel such an approach lends itself well to the current situation in Slovenia, where formal PIAs are not yet commonplace, as it strikes the best possible balance between the thoroughness of the process and the extra administrative burden it places on law enforcement officials. Also, the below-described PIA model has **already been customized for the specific task of evaluating new police powers**.

PIA outline

The Information Commissioner recommends **merging the usual PIA steps** (preliminary phase, identification of risks, identification of solutions to address the risks, delivering the final report) into a consolidated checklist, and then conducting the **proportionality test**.

The goals of such a small-scale PIA include:

- Justified enactment of new police powers, by clearly proving their necessity, adequacy, effectiveness, and proportionality;
- Timely identification of various risks for breaching protection of personal data, "function creep" risks and other related risks;
- Identification of measures to mitigate said risks, such as data minimization, anonymization, use of reasonable data retention periods, use of internal and external oversight, notification of data subjects, etc.
- Grounds for possible regulatory impact analyses (RIAs) with feedback information loop to improve the quality of provisions.

The PIA should include the following steps:

1. The initiating party (generally the Police force or Ministry of the Interior) is to conduct the PIA using these guidelines, and then submit the PIA report to the Information Commissioner for comments;
2. The Information Commissioner reviews the report and submits comments as needed;
3. The initiating party addresses the comments and amends the analysis report if so needed;

[15] For more, see our general PIA guidelines, available at: https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Presoje_vplivov_na_zasebnost.pdf (in Slovene)
[16] Section 208 of the US E-Government Act of 2002 mandates that federal agencies conduct a PIA before commissioning any IT solutions involving processing of personal data. See i.e. the PIA guidelines from the Department of Homeland Security, https://www.dhs.gov/privacy-compliance

4. The initiating party drafts the legislative proposal regarding the new police powers as per the amended PIA, and submits it to the ministry responsible for the Criminal Procedure Law (the Ministry of Justice), along with the remark detailing whether the text respects the comments form Information Commissioner or not
5. The proposal proceeds to the legislative procedure, as usual.

We feel the initiating party is best suited to conduct the PIA, given they have the most information regarding the proposed measures and are thus best placed to assess the risks pertaining to those measures. By bringing in the Information Commissioner into the process, an **independent review** of the whole process is ensured, providing valuable feedback information from data protection experts to the initiating party in order to improve the final legislative proposal. Having that proposal consolidated with the Information Commissioner is a good signal for the competent ministry as well as for the whole legislative procedure.

Conducting the PIA

The main part of a PIA dealing with introduction of new police powers revolves around the timely identification of all involved privacy risks, as well as the safeguards needed to mitigate those risks. Such a PIA should thus incorporate the following four phases[17]:

1. preliminary analysis of the problem at hand;
2. risk analysis;
3. risk mitigation;
4. proportionality test
    a. necessity,
    b. adequacy and effectiveness,
    c. proportionality.

PIA conducted following the above model should provide instrumental information for the drafting of concrete legislative provisions. We now proceed to describe each step in full detail.

1. Preliminary analysis

In this first stage, the initiating party is to explain **why** new police powers are needed, or why existing powers need to be modified. This must include a **detailed account of the problems currently faced by the police**, or explain how the use of new, technologically more advanced measures will allow them to address those problems **in a better and more efficient way.** For example, the initiating party would explain the need for unmanned aerial vehicles (UAVs or drones), and the problems that these UAVs would help them solve.

When proposing new technological measures, the initiating party is to provide a **detailed description of the measures' capabilities**[18], in particular regarding the collection and processing of personal data. This is extremely important with measures that require **judicial oversight** (so that the judge issuing the

[17] In modeling the PIA, we tried to follow the normal legislative process as much as possible.
[18] While providing the make and model can be useful, a general description that includes all the main features should suffice; i.e. »electro shocker, retractable baton, IMSI catcher, drone, …«

warrant can have all the required information in order to make their decision) or the cooperation of third parties (telecommunications or utility companies, etc.).

The preliminary analysis of the situation is followed by a comprehensive **analysis of the risks** involved and the identification of the various solutions and safeguards needed to **mitigate those risks**. Finally, these two stages will serve as inputs for the **three-part proportionality test**.

2. Risk Analysis

As noted above, not all past proposals for new police powers were accompanied by an adequate and detailed explanation, clearly laying out the necessity, adequacy, effectiveness, and proportionality of the new measures. The existing approach, we feel, was war too **casuistic** and incomplete, often focusing only on supposed benefits and completely ignoring accompanying privacy pitfalls. A more optimal approach should include a **timely** and **thorough** assessment of risks associated with possible breaches of subjects' fundamental rights.

In this light identification of the involved privacy risks is essential. It is worth noting that **any risks left unidentified at this stage may later be exposed by both the general and competent public**, possibly even preventing the adoption of the bill. **It is thus in the best interest of the police that all relevant risks are indeed identified at the right time and properly addressed**.

To help we the identification of said privacy-related risks, we recommend using the following checklist.

1. **Risks related to the necessity of the new measure**
    a. Is the use of the new measure / technology truly necessary?
    b. Could the same goal not have been achieved using existing and/or less invasive means? If not, elaborate why.

2. **Risks related to using the new measure**
    a. Risks related to collection of personal data
        i. Risks that the new measures are not adequate for achieving the desired goals?
        ii. Risks that the new measures are not effective in reaching that goal?
        iii. What is the minimal acceptable standard of evidence for considering the use of the measure? Mere suspicion, reasonable suspicion, or even probable cause[19]?
        iv. What are the risks connected with approval procedures - will judges and/or prosecutors understand what technical measure is to be used, what are its capabilities and its implications? How will the new (technical) measures be explained so they can make a truly informed decision regarding the use of the measures?
        v. What are the risks with third parties (i.e. telecommunication companies) that will be required to supply information, or otherwise assist in the use of the measure?
        vi. What are the risks that too much personal information will be collected / that the minimization provisions are not successful?

[19] I.e. have issuing judges been properly briefed on the capabilities and the privacy implications of, say, an IMSI catcher (a device that can capture data on potentially several hundreds or even thousands of persons)?

vii. What are the risks of obtaining false, inaccurate[20], outdated[21], incomplete[22], or irrelevant[23] data?
viii. Will that data actually relate to the persons under investigation, or might it be someone else's data (e.g. data of innocent bystanders, parties in communication etc.)?
ix. What is the extent to which innocent third parties will be subjected to the new measure?
x. How will the effectiveness of the new measure be measured and qualified (justified)? What criteria, benchmarks and indicators will we use to make those assessments?

b. Risks related to the security of collected data

i. What are the risks related to the confidentiality, integrity and availability of collected data[24]?
   1. Risk of access by unauthorized persons?
   2. Risk of abuse by authorized persons? Internal reviews and audits? How will the above breaches be detected and rectified?
   3. Risks that data will be lost, destroyed or altered, breaking the chain of custody?
   4. Risks regarding logging of the use of the measures?
   5. Risks regarding the integrity (non-tampering, non-repudiation) of those logs[25]?

c. Risks regarding the use of collected data

i. What are the risks of collected data not being usable in subsequent criminal proceedings?
   1. Risks of data being incomplete or unverifiable?
   2. Risks with providing due process (particularly the defendant's right of cross-examination)?
   3. Risks regarding the use of data in other investigations (other felonies / misdemeanors)?

d. Risks related to (eventual) deletion of collected data

i. How long will the data be stored, are retention periods appropriate?
ii. What are the risks that irrelevant data is not properly deleted (e.g. with exclusionary DNA samples in DNA-based identification procedures)?
iii. Are there additional costs and risks associated with storing the data?

e. Other risks

i. What are they and what is their impact?

[20] See Matej Kovačič, Trusting digital evidence and traffic data regarding the use of mobile phones, https://pravokator.si/wp-content/uploads/2012/11/Zaupanje_digitalnim_dokazom_in_prometnim_podatkom_v_mobilni_telefoniji_Kovacic2012.pdf (in Slovene).
[21] The Schengen Information System often contains data on cars that aren't considered stolen anymore
[22] Traffic data is of little help in regard to encrypted VoIP services, such as Skype, Whatsapp, Redphone, etc.
[23] Cell tower dumps contain heaps of irrelevant data.
[24] In the context of data protection, data security represents an integral part of data protection.
[25] Log integrity focuses on preventing tampering and other attacks that may undermine the integrity and usability of usage logs (i.e. disabling logging, tampering with existing logs, and destruction of logs). It generally entails use of both technical (SIEM, etc.) and organizational measures (four eyes principle, etc.)

3. Comparative legal research

As part of the risk analysis, existing solutions and best practices of other countries should be considered, especially those of similar judicial and historical environment. The Information Commissioner notes that while existing comparative law explanations are to some extent provided by proponents of the measure, **they tend to focus only on existence and explanation of legal provisions in other countries and not so much on how the measure has fared in practice**, what benefits and drawbacks has it had and how the courts have responded to its use. [26]We find this inadequate, as learning from lessons by other countries through comparative legal research can greatly help in improving the measure, avoiding common pitfalls, and saving valuable time without reinventing the wheel[27].

[26] I.e., a recent proposal for the introduction of police trojans failed to take account of the issues related to the German Staatstrojaner, see http://ccc.de/de/updates/2011/staatstrojaner.
[27] When comparing foreign solutions, cultural, historic and legal differences should be taken into account. The Slovene constitution, for instance, places particular importance on the safeguarding of communications privacy, as a direct response to somewhat widespread government wiretapping and eavesdropping operations done in the former Federal Republic of Yugoslavia.

3. Risk mitigation

After all the respective risks have been identified, one can start addressing them - by modelling various measures and safeguards that help with mitigating the risks.

The use of such safeguards will help to minimize the damage to fundamental rights, prevent the most serious cases of misuse and ensure the admissibility of gathered data in court. They include for example:

- limitations regarding the authorization and use of the measure;
- immediate minimization / deletion of irrelevant data;
- short, well-justified data retention periods;
- measures regarding security of data;
- measures regarding logging / audit trail of data;
- regular reporting and reporting on the use of the measure;
- internal and external auditing;
- due notification of data subject(s), both suspects and innocent third parties;
- etc.

Use of such safeguards will aid in passing the proportionality test (as bellow), and thus help in justifying the use of the measure.[28]

We now detail some of these safeguards, as related to the respective risks they help to address.

1. **Risks related to the necessity of the new measure**
    a. Data, reasoning, comparative legal analyses and other analyses that clearly support the necessity the measure and the inapplicability of other measures.

2. **Risks relating to the use of the new measure**
    a. Risks related to collection of personal data
        i. Data, reasoning and analyses that support the adequacy and the effectiveness of the new measure;
        ii. Justification for the standard of proof that is being used;
        iii. Limitations to use, i.e.
            1. Use limitation to certain or more serious felonies;
            2. Minimization procedures;
            3. Other_____..
        iv. Authorization process
            1. Court warrant, administrative subpoena;
            2. Adequate trainings for investigative judges, police officers;
            3. Other_____.
        v. Solutions guaranteeing the quality of gathered data (completeness, accuracy, timeliness, relevancy, etc.)
            1. Chain of custody,
            2. Control mechanisms[29],

[28] The above list isn't meant as exhaustive. Other measures may apply, as appropriate.
[29] I.e., when using IMSI catchers to determine the suspect's phone number, several readings in several different places should be made, and only the number that's present in all or most of them should be regarded as a possible match.

3. Lessons from follow-up impact analysis (RIA)[30].

vi. Mitigation of risks related to third parties (e.g. when acquiring traffic data)
   1. Clear rules regarding the collection and disclosure of data

vii. Minimization of harm done to suspect (the target of the measure)
   1. Strict rules regarding the target of the measure (no general warrants or "fishing expeditions")
   2. Mandatory judicial approval and oversight (warrants);
   3. Higher standards of proof;
   4. Active minimization procedures (e.g. when wiretapping phone calls)[31];
   5. Mandatory prior/post notification of suspect;
   6. Active participation of suspect, where possible/reasonable.

viii. Minimization of harm done to third parties (collateral damage)
   1. Immediate deletion of irrelevant records, complete with logging;
   2. Anonymization;
   3. Notification;

ix. Defining criteria and benchmarks to evaluate the use of the measure;

x. After-the-fact impact analysis (RIA)
   1. Detailed analysis of the efficiency of the measure.

b. Risks related to the security of the collected data
   i. security measures
      1. Measures ensuring the confidentiality, integrity and the availability of the collected data;
      2. Other.
   ii. logging
      1. Usage logging;
      2. Measures against tampering of logs[32];
      3. (Water)marking copies of paper and electronic data;

c. Risks regarding the use of the collected data
   i. Procedures and manuals
      1. Safeguards ensuring due process;
   ii. Explicit barring of certain uses
      1. e.g. function creep[33];
   iii. Reporting;
   iv. Periodic review (both internal and external);
   v. Other.

d. Risks related to (eventual) deletion of the collected data
   i. Strict adherence to minimal terms of data storage
   ii. Measure for minimization of data after its use
      1. Deletion logs;
      2. Deletion and/or anonymization of unrelated data.

[30] I.e. noting that criminals may be actively engaged in thwarting police surveillance, e.g. by frequently swapping pre-paid phones and /or sim cards, using VoIP not cell phones, using encryption, or possibly even deploying their own cell network.
[31] I.e., the FBI surveillance manual requires agents to stop taping calls if no relevant conversation can be detected some 20 seconds in (see http://www.justice.gov/criminal/foia/docs/elec-sur-manual.pdf).
[32] See note regarding log tampering, as above.
[33] I.e. police trojans (»decoders«) may be used for wiretapping only, and not for forensic analysis.

e. Other risks
    i. Safeguards to tackle other risks.

3. **Comparative legal research.**
    a. Use of safeguards identified through comparative legal research
        i. Best practices
        ii. Court-mandated safeguards
        iii. Additional safeguards due to legal, institutional or cultural differences.

4. Proportionality test

Proportionality test reflects on the information gathered during the previous stages, and seeks to establish that new measures are truly **necessary in attaining their (constitutionally sound) goal**. It entails **usage of concrete, detailed data, reasoning and analysis** that will **clearly show** that the desired goal may not be attained using existing and/or less invasive measures. The latter may not be simply assumed.

As stated, this test is a **three-step process**. First, the necessity of the measure must be proven. Then, the adequacy and effectiveness of the measure must be proven. Finally, the measure must be shown to be proportional in the narrower sense, meaning that its benefits must well outweigh the damage done to fundamental rights of the involved subjects.

4.1 Test of necessity

The test of necessity must show that the proposed measure is **necessary to achieve the aim, that there cannot be any less onerous way of doing it**. This statement must be backed by concrete data, reasoning and other analysis (see example below).

4.2 Test of adequacy and effectiveness

The test of adequacy and effectiveness must show that the **measure is indeed suitable to achieve the aim**, and again **requires concrete evidence** to show it will have that effect. Simply relying on a remote possibility that the measure might be effective (e.g. relying on multiple cell tower dumps to help find the would-be suspect), or relying that the suspect will always behave in some way that will make him easy to find (again, by using his own mobile phone during the commission of a crime) would not suffice.

4.3 Test of proportionality (in the narrow sense)

Finally, the test of proportionality must show that the measure, while already deemed necessary, adequate and effective, must also be **reasonable, considering the competing interests of different groups at hand**. The impact the measure has on an individual's (or multiple individuals') privacy must be compared to the desired benefit for society. A wide-reaching measure (e.g. cell tower dumps, see example as per below) will generally fail to pass such a test, given that police will gain access to

(highly sensitive) mobile traffic data of potentially hundreds of individuals, most if not all of them completely innocent. It may, however, prove to be proportional in some extreme circumstances (missing persons, mass disasters, acts of terrorism).

It is important to note that that the proposed measure **must be able to pass all three of the tests** before it can be tabled for inclusion into law.

In light of the recent mass-surveillance allegations against the United States and some of its allies, the powers of both police and intelligence powers have once again been put on increased public scrutiny. Of particular note is that for most of these powers, there is no to none publicly available information regarding their true scope, further fueling doubts as to their necessity, adequacy, effectiveness, and proportionality. Sooner or later, these doubts will need to be addressed.

Case study – cell tower dump data

To aid in better understanding of the guidelines, we have prepared a case study to show the use of our PIA methodology in practice. The study revolves around a proposed (yet ultimately rejected) change of Article 149.b of the Slovene Criminal Procedure Act (ZKP)[34], one that would allow the police to request traffic data for *whole* cell towers (so-called tower dumps) and not just for individual mobile phone numbers or devices.

The case study is comprised of the usual four steps - an initial assessment, the identification of risks, the mitigation of those risks, and finally the three-part proportionality test.

Note: the study is **meant as an example only**, and should by no means be regarded to be comprehensive and complete. It is just an example of the mental exercise the police is expected to complete before proposing new police powers, to help with future proposals, as they will undoubtedly surface down the line.

1. Initial assessment

Note: in this stage, an analysis into the subject should be done, and main reasons for adopting the new measure are to be outlined.

Example: *In recent years, there have been several cases of industrial theft (mainly copper and similar materials) that the police have thus far been unable to solve. They do, however, believe these cases to be the work of an organized and well-coordinated criminal enterprise, and that that enterprise uses mobile phones as a means of communication for organizing and committing their crimes. An idea has thus surfaced that by obtaining mobile cell tower dumps for the affected regions/times, a list of suspects could be compiled. However, mobile phone operators have been unwilling to provide said tower dump data, stating that the current legislation (Article 149.b of the Criminal Procedure Act - ZKP) only allows for obtaining of data belonging to a concrete mobile phone number.*

In summary, the police provides 10+ cases of such theft with the total damages in the upwards of 250.000€. Use of existing powers, which they believe was thoroughly and properly done, has yielded

[34] See the initial proposal of ZKP-K

no suspects thus far. It is thus their assessment that new (cell tower dump) powers are needed to solve cases such as this.

2. Risk identification

Note: in this stage, possible risks are to be identified, using the checklist as provided above.

Risks related to the necessity of the new measure *relate to the question whether or not these types of crimes truly cannot be solved using existing police techniques. For example, perpetrators of such crimes will usually already be known to the police (repeat offenders with an extensive rap sheet), which means that an initial suspect list probably could be compiled, and then further checked. Also, typical fences that allow for selling of the stolen goods may provide useful information as well. It might be a bit far-fetched to go as far to say that the police simply cannot find any suspects. These types of crimes were quite common in the past - how were they solved back then, when cell phones were not an option yet?*

Risks related to the adequacy and effectiveness of the measure*. It is highly likely the perpetrators will not use mobile phones during the commission of the crime, as they know that may well leave them exposed. And even if they do, they might be using disposable phones or SIM cards which are readily available, helping to hide their identity regardless. Or, they might be using various data services (skype, whatsapp, viber ..) that are not subject to telecommunications data retention at all, or even other communication technologies such as walky-talkies or professional-grade coms equipment.*

Risks related to collection of personal data of innocent third parties*. Cell tower dumps provide data on everyone currently using a specific tower, which could amount to (possibly) several hundred completely innocent people. When granting a warrant for the use of such a measure, this must be taken into account; also, any data on third parties is to be promptly deleted.*

Risks related to the approval of such a measure*. How to properly form an affidavit in support of such a warrant? Is there a risk that judges might simply rubber-stamp such warrants, unaware of the true risks at stake? How will these risks be explained to them in simple, easy to understand terms and who will carry out that task? How should the time frame for which the data is to be obtained, be defined? Also, how should the resulting warrant be written so that* ***third parties*** *(telecommunication providers) have no trouble fulfilling it?*

Risks related to the proportionality of the measure*. The current Electronic Communications Act (ZEKom-1) states that any traffic data sent to the police must be securely kept for as long as 10 years, to ensure its use in the criminal proceedings and to provide an adequate usage regarding the measure. That would mean that a lot of data on a lot of innocent people is kept. This especially so since this data includes information on both those parties using their phones on site of the respective cell tower, as well as the parties they were in contact with, which could be many people from quite far away.*

Risks related to the quality of the data*. As stated, the perpetrators might not be using their phones, or might have left their phones at home, which could render the gathered data unusable for the purpose.*

***Other risks**. Such nigh-unlimited collection of data raises many additional risks, related to information security, internal abuse, use of data for additional purposes, as well as risks and costs associated with proper disposal of acquired data.*

***Comparative law study** should find that this measure is in use in country X and that their police report such and such positive and negative experiences with using the said measure.*

3. Risk Mitigation

Note: The below checklist is meant as an example only, and not as an authoritative list on the matter.

We provide the following data, arguments and analyses in support of the necessity of the measure: _____.

We plan to mitigate the above identified risks using the following measures:

- *Limiting the use of the measure to serious crime;*
- *Use of the measure will be subjected to a prior court warrant;*
- *The procedure for using the measure is to be outlined in detail using an implementation document;*
- *Gathered data is to be analyzed in X days, and any non-relevant data is to be deleted in Y day. Logs for both are to be kept.*
- *Explicit provision prohibiting mining of gathered data for use in other investigations[35];*
- *Use is subject to regular review, both internal (Ministry of the Interior) and external (the Information Commissioner);*
- *Yearly statistics to be provided, clearly reporting the number of cases solved using the data, and the percentage of data that was relevant to those cases.*
- *etc.*

4. Proportionality test

4.1 Test of necessity

We provide the following data, arguments and analyses in support of the necessity of the measure:

Last year, there have been a total of 10 cases related to large-scale theft of copper and other industrial materials. The total damage in these cases is estimated to be upwards of 250.000 euro. The police have thus far, using all existing powers, been unable to produce a suspect. Checking of known suspects, checking with fences, reviewing available video surveillance footage, etc. have all proven to be ineffective. There is, however, a great degree of certainty that the suspects are using mobile devices while planning, coordinating, and executing their crime. It is thus our belief that by obtaining

[35] Due to the number of people affected by the measure, exceptions like the plain view doctrine may not apply.

the cell tower dumps for the respective locations as time periods, and comparing that data, a list of possible suspects could be compiled, and they could finally be brought to justice. We assess that this approach is necessary and justified, given that using all other and/or lesser means have failed.

4.2 Test of adequacy and effectiveness

We estimate the measure to be adequate and effective, even though it includes collecting the data of a large number of possibly innocent subjects. While it is entirely possible that the suspects might refrain from use of mobile devices from time to time, they will eventually need to communicate in this way (it is just too convenient) and once they do, they will get caught. The use of the measure is subject to court authorization, and to strict minimization and logging requirements. This will allow the measure, we estimate, to still be effective, while minimizing the harm to fundamental rights and while maintaining statistical data that can later be used to show that effectiveness in an objective way.

4.3 Test of proportionality

The cases we are dealing with involve serious and organized crime that poses a grave risk to society. That risk, we believe, outweighs the possible harm done to innocent third parties; especially after taking into account all of the proposed solutions for mitigation of the various identified privacy risks.

In summary, given the seriousness of the crime and hand, the urgency to act, the various measures n place to mitigate any and all risks related to privacy, we believe the measures to be proportional, the gathered evidence to be admissible, and that by using the measures the police will be successful in apprehending the suspects of these types of crimes.

Important note

Please observe that the above case study is **meant as a non-exhaustive example only**, and should by no means be regarded to be comprehensive and complete. It serves simply **to illustrate the steps involved in conducting a Privacy Impact Analysis.** It is also worth noting that a well-conducted PIA is only the **first step** in the enactment of new police powers; a step that is expected to be done by the initiating party (generally the police) themselves. Before a conclusive decision on the necessity, adequacy, effectiveness and proportionality of the powers can be made, further steps must be taken, especially regarding the comments made by the Information Commissioner, and by the general public.

Conclusion

In a democratic society, any decisions regarding the use of surveillance technologies **are to be made by the people**, not (just) by law enforcement bodies themselves. Should the latter be the case, then that is not a country ruled by law, but a police state.

The public has the right to be fully informed about all new police powers, and shoulf have theright to critically assess them; if anything, that right only grows stronger as the technology at the heart of

those powers enables the police to collect and process more data than ever before. It is thus in the best interest of the police that any new powers are introduced as transparently as possible, in a manner that will promptly identify any privacy related risks associated with the new powers, provide appropriate safeguards that mitigate those risks, and thus gain acceptance, not rejection, from both the general public and the competent legal authorities.

We believe that these guidelines form but a small piece of that puzzle, and **hope that those proposing new police powers will see that and be inclined to use them as much as possible recognizing it is in their own and common interest to do so.**