Project acronym:	PRISMS
Project title:	The PRIvacy and Security MirrorS: Towards a European framework for integrated decision making
Project number:	285399
Programme:	Seventh Framework Programme for research and technological development
Objective:	SEC-2011.6.5-2: The relationship between human privacy and security
Contract type:	Collaborative project
Start date of project:	01 February 2012
Duration:	42 months

Deliverable 11.3:
The PRISMS Decision Support System

Authors:	Marc van Lieshout (TNO), David Barnard-Wills (TRI)
Reviewers:	Michael Friedewald (Fraunhofer ISI), Gloria Gonzáles Fuster (VUB)

Dissemination level:	Public
Deliverable type:	Report
Version:	1.0
Due date:	31 January 2015
Submission date:	17 July 2015

About the PRISMS project

The PRISMS project analyses the traditional trade-off model between privacy and security and devise a more evidence-based perspective for reconciling privacy and security, trust and concern. It examines how technologies aimed at enhancing security are subjecting citizens to an increasing amount of surveillance and, in many cases, causing infringements of privacy and fundamental rights. It conducts both a multidisciplinary inquiry into the concepts of privacy and security and their relationships and an EU-wide survey to determine whether people evaluate the introduction of security technologies in terms of a trade-off. As a result, the project determines the factors that affect public assessment of the security and privacy implications of a given security technology. The project uses these results to devise a decision support system providing users (those who deploy and operate security systems) insight into the pros and cons, constraints and limits of specific security investments compared to alternatives taking into account a wider society context.

Terms of use

This document was developed within the PRISMS project (see http://prismsproject.eu), co-funded by the European Commission within the Seventh Framework Programme (FP7), by a consortium, consisting of the following partners:

- Fraunhofer Institute for Systems and Innovation Research (Fraunhofer ISI), co-ordinator,
- Trilateral Research & Consulting LLP,
- Dutch Organization for Applied Scientific Research (TNO),
- Vrije Universiteit Brussel (VUB),
- University of Edinburgh (UEdin),
- Eőtvős Károly Policy Institute (EKINT),
- Hogeschool Zuyd and
- Market & Opinion Research International Limited (Ipsos-MORI)

Document history

Version	Date	Changes
1.0	17 July 2015	

CONTENTS

1 INTRODUCTION

The goal of the PRISMS project is to challenge the oft-cited metaphor of the trade-off between privacy and security, and to seek alternatives that better mimic the (complex) interrelation between privacy and security. The alternative approach has been embedded in a Decision Support System (DSS) in which security and privacy are conceptualized from a multidisciplinary perspective in order to enable decision makers to implement security mitigating measures while minimizing the impact on the privacy of individuals and groups. In doing so, this project thus does not see security and privacy as mutually exclusive, but rather as two objectives that often need to be addressed simultaneously and that may influence each other.

The benefit of the DSS for decision makers is therefore a way to take privacy into account in security decision-making. This approach reduces and manages the risk of their security measures causing privacy infringement, with resulting negative impacts for reputation and public perception. Using this approach demonstrates a serious and considered approach to these issues, and decreases the risk of a negative privacy-related outcome. It provides support for meaningful engagement with these issues as part of good citizenship and social responsibility, and shows that the organisation takes these European values and fundamental rights seriously.

This document sets out the PRISMS DSS approach: a document based-process for the systematic consideration of security and privacy in a security investment decision, including participatory elements. The document starts with the basic principles of the DSS, and guidance on the intended audience and intended use. It then provides guidance on using the DSS approach in three contexts: 1) a self-directed approach where a decision maker (the "security investor") works through the questions and templates of the DSS, either by themselves, or with a small internal team in order to structure their own analysis of a security investment decision, 2) a focused approach to structuring exploratory interactive sessions for generating new ideas and perspectives which can feed into security decisions, and finally 3) a comprehensive approach using all the resources of the DSS to fully support the security investment decision. The document contains templates to be used in each stage of the process, and provides annexes containing additional resources.

1.1 BASIC PRINCIPLES

Decision support systems (DSSs) are tools that aim to guide decision makers in the process of making complex decisions and that are based on data and decision-making models. They offer flexibility in the decision-making approach and they can be used by experts and non-experts alike.

The approach of the PRISMS DSS is normative; it has an explicit ethical goal of minimizing the impact on the privacy of individuals of any kind of security measure. This DSS provides insight into the pros and cons of specific security investments compared to a set of alternatives taking into account a wider societal context. This means that the PRISMS DSS specifically takes into account a wider perspective than just that of the problem owner or the stakeholder responsible for making the security investments. The assessment made by the PRISMS DSS is a comparative assessment, in which alternatives are weighted against each other.

It should be noted that the DSS is not an automated decision-making tool itself, but merely a system that guides those who are seeking a broader assessment of potential security measures in such a way that privacy considerations are captured in full. The DSS is essentially a system that is meant to *support* the decision-making process. The result of any activity supported by

the DSS thus is not the final decision on what is the best security investment, but is a presentation of the main findings showing pros and cons, constrains and limits, and alternatives while taking into account the wider societal context.

The DSS is based upon a perspective that is rooted in well-known impact assessment methodologies. Instead of the privacy-security trade-off perspective we adopt an approach in which security and privacy are considered to be separate dimensions with their own value schemes that need to be weighed against each other in an integrative approach. In this manner PRISMS intends to overcome the simplistic assumption that one cannot have both security and privacy when offering safety measures or implementing security devices.

Deliverable 11.1 of the PRISMS project - Background document - provides additional information on the methodological approach and theoretical assumptions about privacy and security underpinning the DSS, including choices made at various stages in the design process, as well as reviewing existing decision support approaches in the area of security and privacy.

1.2 AUDIENCE

The prime intended audience of the PRISMS DSS are security decision-makers responsible for making security investments. Security decision-makers need not necessarily be individuals, but may also be organisational roles or teams of individuals. Examples might include the management team of a transport hub trying to solve the problem of fare dodging, a school attempting to limit access to unauthorised people, or an airport attempting to prevent terrorism.

The second circle of intended audience consists of those that are directly or indirectly linked to the consequences of the security investments and that thus have a stake in what the security solution will look like. This second circle can have a formal role, for instance because of government decision-making that obliges involvement of specific communities or the public at large, and can have a role outside the realm of the security investors (by organising countervailing power against specific decisions). The PRISMS DSS intends to feed and support both perspectives, aiming to achieve the best results in terms of both security and privacy.

The third circle of intended audience consists of public authorities that want to promote a broader societal debate on security threats and potential measures to cope with these threats. Additionally the DSS might be used by other interested organisations that want to explore security measures on privacy impacts.

The second and third circles contribute to the DSS as being a part of participative decision-making. The first circle would profit from including a broader range of stakeholder in the process of decision-making but need not necessarily do so.

In many cases security decision-makers will likely be able to self-identify as such, however some definition of this concept is useful for understanding the primary intended audience of the DSS. In some European languages, security is treated as equivalent to safety, and the PRISMS DSS is designed with this in mind. It can thus be used by decision-makers with responsibilities for public safety. It can be applied to technologies designed for increasing safety, with a particular focus upon methods that use surveillance and other forms of information collection and processing on individuals and populations. It is however not intended for safety in the terms of workplace safety, for example in the prevention of physical injury or accidents.

The PRISMS DSS is intended to support decision-makers in taking security investment decisions in response to security problems. It aims at broadening the scope of decision-making in asking specific attention for the privacy implications of security investments, both at the level of the individual and at the larger societal level. It broadens the set of potential solutions by deliberately searching for alternatives with fewer privacy implications while serving similar security interests. It helps in outlining mitigation measures that reduce negative implications upon privacy and other social rights of specific security measures.

1.3 INTENDED USES

The DSS privacy framework draws upon (but is not limited to) European privacy and data protection law, and to that extent is calibrated for use in the European context. However, to the extent that other jurisdictions mirror European approaches to privacy the approach may be transferable. Additionally, given that the aim of the DSS is not to show legal compliance, those elements based upon the European approach to data protection can be understood as an example of good practice. For further information on the background to the PRISMS DSS approach to privacy and data protection, see Annexes 1& 2

The PRISMS DSS adopts a holistic approach towards privacy and security and starts from a multidimensional perspective on security and privacy that allows a more careful delineation of what the real problem is. It introduces a comparative approach in which the security measure as proposed is confronted with potential alternatives that at first sight have less severe privacy consequences. Elaborating the insights achieved from the research activities of PRISMS (including the survey results) into a DSS that supports decision-making is a real challenge. The PRISMS team made the choice not go for some quick fix but to tackle the challenge in the complexity as it could be present in reality.

The tool itself does not function as a stand-alone tool that can be used off the shelf. It needs involved people who understand the structure of the tool, the structure of the DSS and the various steps that need to be taken. These involved people do not need to be experts or academically trained people. They need management skills in order to guide the process of analysing the various security and privacy issues that are attached to a specific security measure. When needed, they may choose to consult or involve an expert (with a legal background, a criminological background, a policy background, a technological background) depending on the kind of additional information that is needed.

1.4 GLOSSARY

Affected Party - Person or group who may be impacted in some way by the introduction of a security measure. A category of **Stakeholder.**

Decision maker - Person responsible for the decision to adopt, implement or adjust a security measure in response to a security problem. Can also be known as the **Security Investor**

Flow Diagram - Diagram setting out the steps in the PRISMS DSS

PRISMS Decision Support System - A methodology for the structured consideration of privacy and security in a security decision making context.

PRISMS project - EU funded research project into European public attitudes to privacy and security, and the relationship between the two concepts.

Red Flags - A warning system for when issues of significant concern are raised during the decision support system process. May prevent the adoption of a security measure. Can potentially be addressed through mitigating measures.

Stakeholder- Person or group with an interest in the security threat, security measure or measures.

Template - Structured tables with the key questions and issues on which to collect evidence and a way of collecting the answers to those questions. Found in this document from page 16 onwards.

2 USING THE DSS

As discussed in the introduction, the PRISMS DSS can be used to support security investment decisions in three contexts. For each of these contexts, this section provides a description of the context, an overview of the advantages and disadvantages of this particular mode of use. Each set of guidelines then indicates which templates from the full set should be used in that mode, and which can be omitted from the process.

Using the DSS primarily involves providing answers to series of questions. These questions are based upon research in privacy and security, and are structured to tease out some of the complexities of decisions in this field. By the end of the process, the answers that have been provided will help the decision maker to come to an informed and considered decision, and also to provide a report of the structured process that led to this decision.

2.1 GUIDELINES FOR SELF-DIRECTED USE

This section provides guidance for the use of the DSS by a security decision maker either on their own or supported by an internal project team. This version does not include the participatory elements of the full DSS, but still provides a methodology for the structured consideration of privacy dimensions within a comparison of security measures.

When selecting this approach, the following advantages and disadvantages should be taken into account:

Self directed use of the PRISMS DSS	
Advantages	Disadvantages
Quicker than full process	External perspectives may still be gathered, but this will be through proxies and general information (for example, opinion surveys) rather than collecting new information specifically targeted to a particular measure in response to a particular threat in a particular context.
Desk based	Decision makers may not fully understand and therefore not be able to fully represent the perspectives of affected parties.
Can be handled internally within an organisation	Additional and unexpected insight that make come from including external experts and affected parties will be missing
Lower organisational burden (no organisation of workshops and focus groups) and therefore requires a smaller number of people.	Use in this manner does not create as much transparency as a participative process, although reports emerging from this process might still be made public or available to regulators.
Can be used in an exploratory fashion for potentially sensitive issues	Similarly, this process may appear less legitimate to interested publics and affected parties. They may wish to have been included
More suitable **if** security risks will inherently occur from engaging affected parties (although this should not be a starting assumption and should be evidenced in the account of the security threat).	

The PRISMS DSS provides several moments where input from stakeholders should be sought to increase the quality of the data gathered to support the decision. It is possible to functionally complete these sections with only the input from the problem owner or project team, but the end result will be more limited, less informative, more partial and potentially less legitimate than a process that has included a wide range of stakeholders and impacted parties in the evidence gathering.

Example 1: NGO explores surveillance features of use of drones with facial recognition capabilities in demonstrations

The police in a big city have announced it will start using drones for the monitoring of demonstrations. It will not use the drones for all demonstrations but only in situations when the police consider the threat on violent extension of the demonstration to be within reasonable expectations. The drones will have cameras with sufficient resolution to enable facial recognition at the back end side. A national NGO decides to confront the plans of the police with the PRISMS DSS. It does so by following the first two stages of the DSS in full. It identifies alternative measures that help in addressing the security threat. It aims at identifying red flags. It does not feel the need to explore mitigation strategies in order to improve the approach chosen by the police. In the reporting phase it pays attention to rebound consequences and systemic impacts.

Templates to use in self-directed mode	Notes
Preparatory Phase	
4.1 Chance of occurrence of the threat 4.2 - Impact of the threat 4.3 - Measures proposed to counter the threat 4.4 - Effectiveness of measures proposed 4.5 - Alternatives to proposed measures 4.6 - Available evidence on attitudes, perspectives and behaviour related to security measures	Consultation with external parties (either external experts, stakeholders or affected parties) is suggested in the full version of the DSS approach, particular to help with the generation of alternatives to a proposed security measure in step 4.5. This may be lacking in this approach. Similarly, 4.4 has a question about if the effectiveness of a security measure is contested. This information might also be more difficult to obtain in this manner. In this self-directed mode the burden of creating or selecting additional measures is placed upon the decision maker, and upon any available research on the topic of public attitudes to the security measures proposed.
Assessment Phase	
5.1 - The fundamental conditions for privacy 5.2 - Potential infringement of privacy 5.3 - Potential infringement of the right to the protection of personal data	The PRISMS DSS provides several moments where input from stakeholders should be sought to increase the quality of the data gathered to support the decision. It is possible to functionally complete these sections with only the input from the problem owner or project team, but the end result will be more limited, less informative, more partial and potentially less legitimate than a

Templates to use in self-directed mode	Notes
5.5 - Additional requirements 5.7 - Summarising the impacts	process that has included a wide range of stakeholders and impacted parties in the evidence gathering.
Mitigation Phase	
6.1 - Inventory of red flags and possibility of mitigation 6.2 - Can the system be reconfigured to better meet data protection principles 6.3 - Mitigating long term impacts 6.4 - Summary of mitigation measures	The mitigation phase starts with the identification of so-called red flags. This presupposes willingness on the side of the party performing this exercise to acknowledge the presence of red flags. It also presupposes willingness to acknowledge opportunities for improving the system through application of data protection principles.
Reporting Phase	
7.1 - Pros and cons of the measures 7.2 - Constraints and limits 7.3 - The wider social context 7.4 - Final conclusions	Depending upon internal requirements, the reporting phase may not be necessary, as the relevant aspects of the decision may have been sufficiently highlighted for the decision makers, you may not need to do the reporting phase.

Templates to omit from the self-directed use
5.4 - Individual, group and categorical impacts and experiences should be omitted, because these questions are primarily directed at groups other than the decision maker/security investor and therefore cannot be adequately answered by the decision maker alone. 7.1 - Pros and Cons - the section on the pros and cons for affected parties may be difficult to complete for the same reasons. 7.2 - Constraints and Limits - may be replaced by appropriate internal processes and policies of the security investor However, this section may be used to record some of these constraints and their investigations to keep this in the same place as the privacy and security analysis.

2.2 GUIDELINES FOR EXPLORATORY USE

The DSS can be used to support the exploration of emerging security technologies; new applications or situations in which novel surveillance oriented security technologies are foreseen. This can be done in a stage in which it is foreseen that novel applications and systems will be developed and introduced, in order to promote an early discussion on these applications and systems. Security investors could be interested in having this *ex ante* assessment in order to have an early perspective on potential pitfalls or barriers. NGOs could be interested in performing such an exercise in order to explore in a systematic and structured manner emerging technologies and applications at an early stage. It also might help them in exploring applications or situations to which they would like to respond.

Exploratory use of the PRISMS DSS	
Advantages	Disadvantages
Enables a systematic and structured analysis of situations or emerging trends 'just to familiarize oneself' with these situations or trends.	Limited legitimacy of results ('just a brainstorm or creative exercise'; 'no real connection to reality').
Offers the opportunity to explore a broader range of alternatives.	Restricted participation of stakeholders.
Can be organised as a 'light' exercise, in a relatively short period of time.	Can lead to reinforcement of already existing prejudices and assumptions.
Low organisational burden.	Can lead to exploring security threats that are not recognisable to other stakeholders as relevant or sufficiently realistic.
Opportunity to construct the threat situation to be explored.	

Depending on the intention of the actor performing the exploratory exercise and the resources available to this actor (time, money, available expertise) a specific routing through the Decision Support System will be taken. In order to highlight the breadth and variety of the approaches that can be chosen, we present two typical situations in which an exploratory exercise can be chosen: one in which an NGO sets itself at exploring potential new security threats that it identified, and another in which a security investor wants to perform a kind of quick check on potential pitfalls in implementing new surveillance oriented security technologies.

Example 1: NGO starts investigating the use of biometric data for surveillance purposes.

A nationwide NGO has decided to use the PRISMS DSS to explore the potential use of biometric data for surveillance purposes. It organises a series of workshops in which it invites experts and citizens to discuss privacy implications of the approach and explore opportunities to address the most obvious infringements and to mitigate these. It wants to engage policy makers in a societal debate concerning these developments since these developments are 'creeping upon society'. The NGO considers the PRISMS DSS to offer an interesting inroad to this discussion given the fundamental approach chosen and the option to explore alternatives as well. The final result of the NGO's approach is a report that presents its findings and that is summarized in a number of short media presentations.

Example 2: Security investor explores potential of new security measures

An internationally operating security investor has decided to use the PRISMS DSS to explore the potential pitfalls of some new security developments as part of the design phase. It wants to explore the use of smart algorithms in surveillance systems in order to lower the need for security personnel and to enhance the effectiveness of the surveillance system in detecting abnormal behaviour in public places (pick pockets, small riots, traffic problems). It organises a process in which it explores the privacy implications of the new system and in which it discusses a number of alternative strategies in having smartness introduced in the system. It uses the PRISMS DSS because of its approach that starts from a number of fundamental assumptions with respect to privacy and its flexibility in having this tested together with a number of alternatives. Though it organises the process as an internal process, the firm

invites a number of experts to discuss the issues and to have a broader perspective on potential mitigation strategies.

These illustrations point at the various approaches in which the PRISMS DSS could be used. While the first illustration emphasizes the need to roll out the results to a wider audience and thus will pay attention to the wider societal context and potential rebound effects, this will not be a part of the second approach. One apparent risk in the exploratory approach is that – while referring to the encompassing approach the PRISMS DSS presents – organisations will only use these parts of the approach that helps emphasizing their own interests. The advantages that are offered through the approach of the PRISMS DSS (taking into account alternatives, starting from a fundamental perspective but including concerns as well, offering an inroad to mitigation strategies) can be exploited but cannot be enforced.

Templates to use in exploratory mode	Notes
Preparatory Phase	
4.1 - Chance of occurrence of the threat 4.2 - Impact of the threat 4.3 - Measures proposed to counter the threat 4.4 - Effectiveness of measures proposed 4.5 - Alternatives to proposed measures 4.6 - Available evidence on attitudes, perspectives and behaviour related to security measures	Consultation with external parties (either external experts, stakeholders or affected parties) is suggested in the full version of the DSS approach, particular to help with the generation of alternatives to a proposed security measure in step 4.5. This may be lacking in this approach. Similarly, 4.4 has a question about if the effectiveness of a security measure is contested. This information might also be more difficult to obtain in this manner. However, one could also expect a more in-depth exploration of possible alternatives given the exploratory character of the approach.
Assessment Phase	
5.1 - The fundamental conditions for privacy 5.2 - Potential infringement of privacy 5.3 - Potential infringement of the right to the protection of personal data 5.4 - Individual, group and categorical impacts and experiences 5.5 - Additional requirements 5.6 - Summarising the impacts	The PRISMS DSS provides several moments where input from stakeholders should be sought to increase the quality of the data gathered to support the decision. It is possible to functionally complete these sections with only the input from the actor that is performing the exploratory exercise, but the end result will be more limited, less informative, more partial and potentially less legitimate than a process that has included a wide range of stakeholders and impacted parties in the evidence gathering. Depending the background and interest of the actor performing the exploratory exercise, attention for specific aspects could be reduced.
Mitigation Phase	
6.1 - Inventory of red flags and	The mitigation phase starts with the identification

Templates to use in exploratory mode	Notes
possibility of mitigation 6.2 - Can the system be reconfigured to better meet data protection principles 6.3 - Mitigating long term impacts 6.4 - Summary of mitigation measures	of so-called red flags. This presupposes willingness on the side of the party performing this exercise to acknowledge the presence of red flags. It also presupposes willingness to acknowledge opportunities for improving the system through application of data protection principles. Interest in measures to mitigate long-term impacts may vary depending on the background of the actor performing the exercise.
Reporting Phase	
7.1 - Pros and cons of the measures 7.2 - Constraints and limits 7.3 - The wider social context 7.4 - Final conclusions	Depending upon the intention of the actor performing the exploratory exercise, attention for the reporting phase may be limited, but may also be crucial.

One cannot predict in advance which templates will and which templates will not be used in an exploratory exercise. Depending on the actor that has the lead in the exercise and on the involved parties, some issues will be more difficult to address.

In some of the questions posed in the preparatory phase section on security measures , it is presumed a security investor is available. This will not always be the situation. In civic panels discussing potential measures without direct intervention of or interaction with a security investors, these questions could be skipped (question 4.3 and 4.4 may be hard to answer without a responsible security investor present in the panel, while question 4.5 may be hard to answer as well).

When attention is foremost oriented towards exploring new uses or new developments with the aim of organising more awareness and/or public debate, the mitigation measures that help exploring systems reconfigurations may be less relevant (question 6.2). On the other hand, when the exploration is dedicated to exploring new measures within the circles of the security investor, attention for the wider societal and longer-term implications (questions 6.3) may be less relevant.

The regrouping of the findings in terms of pros and cons, constraints and limits and the wider social context (question 7.1, 7.2 and 7.3) will depend as well on whose interests are at stake. In the first illustration offered, these questions may be crucial, while in the second illustration offered they may be hardly relevant.

Templates to omit from the exploratory mode use
Situation dependent. See explanation above

2.3 GUIDELINES FOR COMPREHENSIVE FULL-SCALE USE OF THE DSS

This section provides guidance on the full-scale use of the PRISMS DSS. As might be expected, the comprehensive approach makes use of (potentially) the full set of templates and questions provided in this document. It also includes an appropriate amount of participatory methods and evidence gathering.

Comprehensive use of the PRISMS DSS	
Advantages	Disadvantages
Complete coverage - The DSS has been designed based upon cutting edge research into security and privacy. The elements that are included in the DSS are there so that the complexity of the privacy dimensions of a given security threat and security measures can be fully considered and that all significant dimensions can be taken into account. Removing or passing over elements of the DSS offers the risk that important issues can remain undiscovered. Adopting a comprehensive approach makes the best use of the insights supporting the DSS as well as the greatest change of unearthing privacy issues before they become problematic.	Time - the biggest disadvantage of the comprehensive approach is that it requires more time to go through all the stages, and particularly to involve external participants such as experts and stakeholders. If this approach is to be adopted, it should be adopted far enough in advance of the desired or intended implementation of the security measure to allow for the complete process. The length of the process is, however, dependent upon the particular security context, the complexity of the security threat and measures, and the availability of external participants and their willingness to participate in the process. This is best assessed by the decision making in the initial stages of planning a project using the DSS approach.
Thoroughness - The decision maker can demonstrate that they have adopted the approach in its fullest and that they have made a serious consideration of all elements. They are also free from accusations that they have omitted potentially troublesome sections so as to achieve results that they prefer.	Cost - in a similar manner, the comprehensive approach involves more people, requires more organisational effort and greater resources to bring to completion.
External input and perspectives are most fully incorporated in the comprehensive approach. These perspectives can by extremely valuable for understanding privacy impacts which may not be apparent to the decision maker, no matter how concerned they are with reducing negative impacts.	Creation of involvement and ownership - involvement of external participants in this process can lead them to develop a sense of ownership over the process. Whilst this level of engagement is positive, it does bring a responsibility to treat these participants honestly and openly and not to take their input in vain. This can be burdensome for the decision maker and they should put planning in case for this situation.

For the comprehensive use of the DSS, the decision maker, and any supporting experts progresses through the stages of the DSS. The broad phases (Preparatory, assessment, mitigation and report) should be addressed in order, although some information relevant to other phases can be surfaced at various points. It is therefore worth the user familiarising themselves with the templates for various sections as they are planning to use the PRISMS DSS approach. The templates within the sections can be ordered more flexibly, and it might be possible to run various elements in parallel, especially if waiting for research efforts to produce answers, or for participatory methods to be sufficiently organised.

Example: Public authority addressing anti-social behaviour in mixed-use public space

A local authority with responsibility for public safety in a mixed use public space (some local business, public amenities and transport infrastructure) seeks to respond to the anti-social behaviour (graffiti, noise, litter). The threat is common but of low impact. It is initially considering installing security cameras, but is concerned that these might be ineffective and might have privacy implications. It compares this measure against two alternatives, street-based workers from the local authority or security guards from a private company. In assessing the impacts it organises consultation sessions with local resident and business stakeholders, including young people. It finds that whilst people are concerned about their privacy, they also feel that a human security presence can also be troublesome, with a higher potential for discrimination. However residents generally prefer the local authority-employed street workers to private security guards, seeing them as more legitimate and more publicly beneficial. The mitigation stage identifies some technological and procedural measures which can be employed to reduce the privacy impacts of CCTV and procedural rules for the workers to follow in interacting with the public.

Templates to use in exploratory mode	Notes
All templates in this document (Sections 3 to 7)	
Templates to omit from the exploratory mode use	
None (however, some templates may be less relevant for particular threats and measures and can therefore be completed at a lower level of detail).	

Flow diagram for comprehensive DSS

Preparatory Phase (I)					
Chance of occurrence of the threat	Impact of the threat	Measures proposed to counter the threat	Effectiveness of measures	Alternatives to proposed measures	Evidence on attitudes

Assessment Phase (II)					
The fundamental conditions for privacy	Potential infringements of privacy	Potential infringements of the right to protection of personal data	Additional requirements	Individual, group and categorical impacts	Summarising the impacts

Mitigation Phase (III)			
Inventory	Reconfiguration for privacy principles	Mitigating long term impacts	Summary

Report (IV)			
Pros and Cons	Constraints and limits	Societal Context	Final conclusions

3 PRISMS DSS TEMPLATES

The following sections provide the question templates for the PRISMS DSS. These are also available in an associated Excel spreadsheet. This spreadsheet provides some additional functionality such as links between templates, and some automatic filling of repeated fields.

The spreadsheet can be downloaded from: http://prismsproject.eu/?p=378

The following figure shows the overview of the various activities that are part of the PRISMS DSS process. The figure shows that the entire process captures four phases:

a. A preparatory phase
b. An assessment phase
c. A mitigation phase
d. A reporting phase.

The preparatory phase is focused upon preparing the material for the assessment phase. It is composed of a number of building blocks that starts with getting a proper view of the threat that needs to be countered. It continues with inventorying the security measures that are proposed to counter the threat. Special attention is given to what is known about the effectiveness of these measures. Alternative measures are sought for. These measures should be genuine alternative measures, meaning that they are sufficiently mature and robust to offer a realistic alternative to the security measures as originally proposed. For all measures available evidence will be collected on various aspects of the measures (effectiveness, acceptability by involved citizens, costs).

The assessment phase starts with assessing the potential infringements of fundamental rights. This relates to legitimacy, suitability and necessity of the measures proposed. To indicate a serious drawback, red flags are used in this phase. The second step is an assessment of the privacy implications. Finally, the assessment inventories how affected persons/groups of persons perceive the impact of security measures.

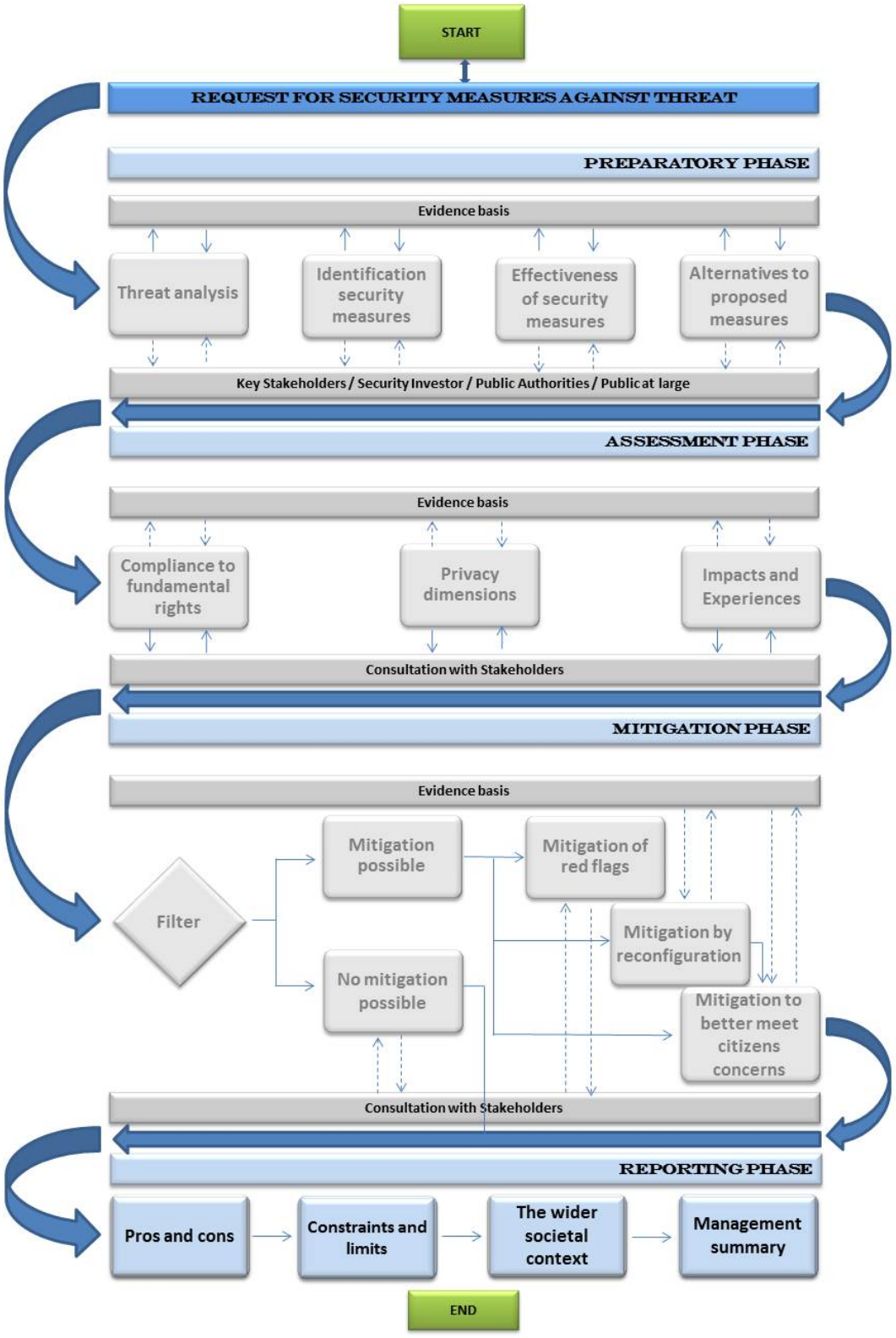
In the third phase, the negative consequences that have surfaced will be checked for opportunities to mitigate them. A first check will be done on whether the measures proposed are open for mitigation, and whether they contain red flags that might be prohibitive for the measure as such. Then it will be checked what kind of mitigation measures can be used to improve the measure.

The final phase is the reporting phase in which all elements that have been gathered will be presented. The presentation starts from the requested analysis: pros and cons, constraints and limitations and the wider social context. Finally, a management summary will be produced.

During all phases, stakeholder consultation (in the form of working group meetings, conferences, focus groups, interviews, surveys, etc.) can be part of the approach. This is indicated in the flow chart by the arrows oriented to the bottom of each phase. Usually, consultations will depend on time and resources, and on the scope of the measures to be explored. Similarly, it will be possible to consult an evidence base in each phase. This evidence base is a base that needs to grow over the years. PRISMS presumes that the results of PRISMS and its counterparts SurPRISE and PACT, form a first resource of information and evidence that can be consulted.

Finally, although this is not explicitly indicated in the flow chart, the building blocks per phase do not have to be executed in a strict sequential order. In practice, it might be necessary to jump a bit forward and backward. The preparatory phase will also yield some information

that is very useful for the assessment phase. As such the flow chart and the structure proposed function as a guiding device and not as an obligatory menu to be swallowed.



4 PREPARATORY PHASE

The first phase in the DSS is the preparation of the input so that it enables the execution of the impact assessment. In the preparatory phase questions are posed that help identify characteristics of the security threat and of the proposed security measures, including surfacing assumptions and background knowledge about the nature of the threat and why it requires a response. It will also help in the further assessment of potential additional measures that can be implemented, in order to deal with the identified security threat.

The PRISMS DSS takes a societal context as a starting point. In the vignettes that PRISMS has used to search for the various privacy and security aspects of these societal contexts, these contexts can be virtual or physical (or a mix), can have public or private main actors (or a mix) and can address various privacy and security dimensions. The preparatory phase will help identifying the specifics of the threat and the proposed measures in terms of these dimensions so that experience with the vignettes can be invoked where needed.

The preparatory phase consists of the following steps:

1. Chance of occurrence of the threat
2. Foreseen impact of the threat
3. Measures proposed to counter the threat
4. Effectiveness of measures proposed
5. Alternative to proposed measures
6. Available evidence on attitudes, perspectives and behaviour relating to security measures.

Many questions in the preparatory stage are meant to support the assessor in finding the appropriate level of investigation of the threat that is being responded to. Therefore answers in this section can be relatively succinct.

Template used in:					
Self-Directed	Yes	Exploratory	Yes	Comprehensive	Yes

4.1 CHANCE OF OCCURRENCE OF THE THREAT

4.1.1 Rationale

In order to evaluate whether a threat needs to be taken seriously, two dimensions are evaluated:

1. The chance an event occurs
2. The impact of an event when it occurs

Together, this adds to the simple and straightforward approach of a security risk as being the product of the chance that a threat occurs times the consequences of that threat. This gives rise to well-known impact matrices that bring together the chance of an event and the impact of the occurrence of the event.

As indicated in this matrix, frequency of occurrence over time flows from unlikely to frequent while severity runs from negligible to catastrophic. While in some (engineering) fields it will be possible to present quantitative figures for frequency of occurrence (for example the probable failure rate of a technological component) and for the grade of severity, when it comes to more diffuse security threats, this will be more problematic and this form of quantitative analysis usually is not possible. In the templates, a different scaling is used (continuous, predictable, incidental) that may help characterizing the chance of occurrence of the threat

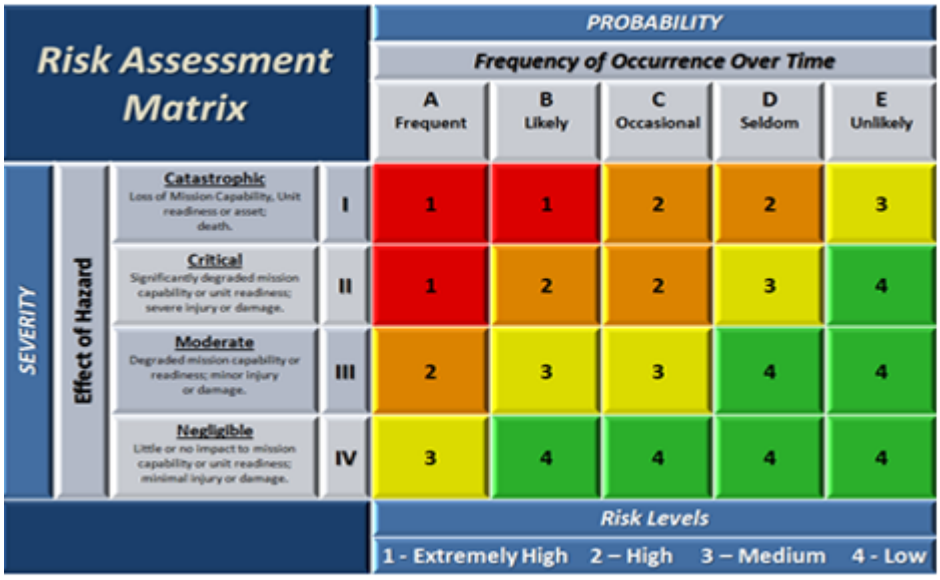


Figure 1: Risk assessment matrix (www.airforcevirtualwingman.com)

4.1.2 Guidelines

In order to determine the chance of occurrence of a threat, the DSS first asks to provide some general information on the threat and then continues by asking for some more detailed information that helps determining the relevance of the occurrence of the threat.

4.1.3 Action

Answer the following questions, and record the answers.

Question	
Please, describe the security threat for which security measures are warranted.	[Use the following sub-questions: 1. Could you describe concisely, in one or a few sentences, the threat? 2. Could you indicate in general terms the dimensions of the threat (physical/non-physical threat, local/virtual, technological/non-technological, …)? 3. Please describe any other unique characteristics of the threat.
Please, describe the occurrence of the security threat	[Use the following sub-questions: 1. Does the security threat pose a continuous threat? (such as 'the war on terror', or a virus threat on the internet) 2. If not, does it pose a regular threat that occurs every now and then on a more or less predictable basis (cf. demonstrations, hooliganism, speeding) 3. If not, does it pose a threat that is usually rather incidental, i.e. with a low chance of incidence (cf. parents/people kidnapping children at school, …) 4. Add any other information concerning the occurrence of the threat you consider relevant.
Please, present more information on the occurrence of the threat.	[Use the following sub-questions: 1. What evidence is available for the likelihood of occurrence of the threat? Please provide the sources of evidence if possible. 2. Why are you, as a security decision maker, responsible for responding to this threat? (examples might include legal responsibility, political attribution or pressure, public opinion, moral obligation, ownership of threatened assets, and pressures from technological developments). Please provide details.

Table 1: Chance of occurrence

Template used in:					
Self-Directed	Yes	Exploratory	Yes	Comprehensive	Yes

4.2 IMPACT OF THE THREAT

4.2.1 Rationale

The second dimension of the threat to assess is the impact it causes. This is also known as the severity of the threat. The impact determines whether specific measures to counter the threat are warranted. A security threat with a high impact might warrant more radical measures to counter the threat than a rather modest security threat (still taking proportionality of responses and presence of less radical responses into account). For the kinds of security measures that the DSS tackles, it will usually be difficult to present any quantitative assessment of the impact of the threat. Still, in setting the scene, some information on the impact of the threat can be collected. This information will help in developing a clearer picture of the threat and assessing the security measures that are announced to counter the threat.

This section also asks the audience of the DSS (decision maker, public authority, public at large) to briefly consider the privacy implications (if any) of the threat. This may be readily apparent in some cases (for example, the threat of unauthorised access to personal information stored on a database) but less obvious in other cases.

4.2.2 Guidelines

In PRISMS, security is seen as comprising a broad range of dimensions. PRISMS not only captures physical security but takes other forms of security into account as well, such as cultural security, and radical uncertainty security (see box 1 below for concise descriptions of these dimensions). It is important to evaluate the impact concerning the security dimensions that are at stake in the security threat. It is also important to address the scope and characteristics of the people affected by the threat. The questionnaire differentiates between people directly affected by the threat, and those indirectly affected. Finally, this template also asks you to identify any privacy dimensions that are invoked by the security threat. To give an example, in case of a threat that may cause bodily harm, privacy of the body is at stake. Additional information on the concept of privacy in the PRISMS DSS can be found in box 2.

4.2.3 Action

Answer the following questions, and record the answers.

Question	
How would you describe the impact of the threat in terms of: 1. people affected? 2. Groups of people affected? 3. Categories of people affected? 4.2.4 (Explanation of difference between	[Use the following sub-questions: 1. Which people are directly or indirectly affected by the security threat? Which groups of people are directly or indirectly affected by the threat? Which categories of people are directly or indirectly affected by the threat? 2. Is the group/category of directly/indirectly affected people well-defined? 3. If not, is it possible to describe the group/category of directly/indirectly affected people? 4. Can you indicate the scope and size of the (group of) people affected? a. Very substantial – substantial – small – very small – indefinite

<table>
<tr><td>Question</td><td></td></tr>
<tr><td>groups of people and categories of people)</td><td>b. Very targeted – targeted – non-targeted – indefinite
c. Belonging to the same territory – international – virtual</td></tr>
<tr><td>Could you describe which sorts of security impact are the most relevant for the affected people?</td><td>[Use the following categorisation:
Does the security threat have an impact upon:
1. Physical security
2. Cyber/Informational security
3. Socio-Economic security
4. Radical uncertainty security
5. Political security
6. Cultural security
7. Environmental security

How would you evaluate the kind of impact it has on these dimensions?
a. Very substantial – substantial – small – very small – indefinite

<table>
<tr><td>Security type/extent of impact</td><td>Indefinite</td><td>Very small</td><td>Small</td><td>Substantial</td><td>Very substan</td></tr>
<tr><td>Physical</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Cyber/Informational</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Socio-economic</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Radical uncertainty</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Political</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Cultural</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Environmental</td><td></td><td></td><td></td><td></td><td></td></tr>
</table>

Please provide additional information if considered necessary to indicate how the threat impacts the various security dimensions. This information might be obtained from looking at incidents of this threat or similar related threats in similar and related contexts.</td></tr>
<tr><td>Does the threat evoke or imply any privacy implications?</td><td>[Please, describe in your own terms the privacy implications of the threat, if any. You can use the privacy dimensions in use within PRISMS:
1. Privacy of the person
2. Privacy of behaviour and action
3. Privacy of communication
4. Privacy of data and images
5. Privacy of location and space
6. Privacy of association (including group privacy)
7. Privacy of thoughts and feelings</td></tr>
</table>

Table 2: Impact of threat

Box 1: Explanation of security dimensions

Physical security: That part of security concerned with physical measures designed to safeguard the physical characteristics and properties of systems, spaces, objects and human beings.

Information and cyber security: That part of security concerned with measures designed to protect information, information systems and communication infrastructures from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.

Socio-economic security: That part of security concerned with economic measures designed to safeguard the economic system, its development and its impact on individuals.

Radical uncertainty security: That part of security concerned with measures designed to provide safety from exceptional and rare violence/threats, which are not deliberately inflicted by an external or internal agent, but can still threaten drastically to degrade the quality of life.

Political security: That part of security concerned with the protection of acquired rights, established institutions/structures and recognized policy choices.

Cultural security: That part of security concerned with measures designed to safeguard the permanence of traditional schemas of language, culture, associations, identity and religious practices while allowing for changes that are judged to be acceptable.

Environmental security: That part of security concerned with measures designed to provide safety from environmental dangers caused by natural or human processes due to ignorance, accident, mismanagement or intentional design, and originating within or across national borders.

Box 2: Explanation of privacy dimensions

Privacy of behaviour and action: that part of privacy that deals with the right to protect sensitive issues such as sexual preferences and habits, political activities and religious practices, collected either by casual observation by a few nearby people or through systematic recording and storage.

Privacy of communication: that part of privacy that deals with the protection against the interception of communications, including mail interception, the use of bugs, directional microphones, telephone or wireless communication interception or recording of email messages.

Privacy of data and image: that part of privacy that deals with the protection of an individual's data from being automatically available or accessible to other individuals and organisations and that enables people to "exercise a substantial degree of control over that data and its use".

Privacy of location and space: that part of privacy that deals with the protection of the right to move about in public or semi-public space without being identified, tracked or monitored.

Privacy of association: that part of privacy that deals with the right to associate with whomever one wishes, without being monitored.

Privacy of thoughts and feelings: that part of privacy that deals with the protection of the right not to share one's thoughts or feelings or to have those thoughts or feeling revealed.

Template used in:					
Self-Directed	Yes	Exploratory	Yes	Comprehensive	Yes

4.3 MEASURES PROPOSED TO COUNTER THE THREAT

4.3.1 Rationale

Having inventoried relevant characteristics of the threat, the DSS now turns to inventorying the measures that are under consideration for countering the threat. Each specific threat (for example the threat of hooliganism) may evoke a set of measures to counter it. The measures can be characterised as predominantly technological, organisational or socio-political. The measures can have an impact on (one or more dimensions of) privacy. The challenge of the DSS is to explore the privacy implications of specific measures and to search for the best solution possible. To that end, the first step is identifying the measures, analysing specific features of the measures, scoring their effectiveness (if known) and checking for alternative measures. The in-depth evaluation on the privacy implications of the measures will be part of the impact assessment phase. In the preparatory phase the measures will be inventoried on some other basic constraints.

4.3.2 Guidelines

In this stage, the measures will be inventoried on a number of dimensions that inform about the specificities of the measures. Depending on the kind of threat, usually there will be a set of measures, instead of a single one. The inventory will be performed for each measure, while measures should be grouped in order to minimize work on the inventory as much as possible. Measures can be primarily technology oriented, organisation oriented or socio-politically oriented.

The measure itself may confront a large number of people or only a few. Again, scoring the impact of the measure on this aspect is highly contextual. The perceived impact of a surveillance camera in a busy shopping centre could be higher than the surveillance of Internet traffic of billions of people.

The (financial, organisational) investments to be made in order to install the measure give some information on the flexibility of the measure. When investments are large and flexibility in the measure is modest, it will probably be a measure ‘here to stay’. If the measure requests large organisational investments but relatively minor financial investments (organising surveillance activities in a different manner) it may be revoked if specific circumstances demand this.

In some of the questions posed hereunder, it is presumed a security investor is available. This will not always be the situation (for instance in civic panels discussing potential measures without direct intervention of or interaction with a security investors). These questions could be skipped (question 3, 4, 5 may be hard to answer without a responsible security investor present in the panel).

4.3.3 Action

Answer the following questions, and record the answers.

Question	
Which measures are foreseen to counter the threat presented in the previous section?	Provide a concise description of the security measure to be explored: Score each measure on the following features: 1. Is the measure mainly a technological/organisational/socio-political measure (see guidelines)? 2. Would you consider the measure to be well understood in how it works? 3. Does the intended investor have previous experience with the measure (see guidelines)? 4. Will the measure be delivered and controlled by the security investor or by a third party? 5. Will the measure be overseen by the security investor, by some independent authority, or will it be implemented without oversight? 6. Does the measure affect a large group of people (see guidelines)? 7. Does the measure require large investments/relatively modest investments? 8. Is the measure easy to revoke or will it be difficult to modify or reverse the measure? 9. Has the measure been previously deployed for this purpose in other related contexts? Please, explain your choice.

Table 3: Security measures to counter the threat

Box 3: Modes of measures

A **technological** measure is a security measure in which a technological system or component is necessary for the measure to be effective. Using CCTV to notice aggressive behaviour at the street is an example. Monitoring Internet traffic in order to check for malevolent connections is another.

An **organisational** measure is a measure in which an adaptation within an organisation or between organisations is necessary to accomplish the measure. This could for instance be the implementation of an access management system in order to track that is present in a specific part of a building or premises.

A **socio-political** measure is a measure that has a political dimension (such as a law, a regulation or a verdict) or that has a civic/private dimension (such as a neighbourhood watch).

Template used in:					
Self-Directed	Yes	Exploratory	Yes, but depending on context	Comprehensive	Yes

4.4 EFFECTIVENESS OF MEASURES PROPOSED

4.4.1 Rationale

One of the most critical aspects of evaluating a measure is to assess whether it is effective yes or no. Scoring the effectiveness however presumes a thorough framework to define the criteria against which the effectiveness of a measure can be evaluated. If a measure fails to pass an effectivity test, it is no use implementing the measure. If properly done, an ex-ante effectiveness assessment should be done, followed by an ex-ante or ex-post measurement (to check for any inconsistencies, and to enable learning by doing).

One way to assess the effectiveness of the measure is by looking for similar situations and checking how the measure functioned in that situation. This requires the ability to define the criteria that are similar (or rather similar) in both situations. Gathering evidence on similar (or rather similar) measures in similar (or rather similar) situations can offer a better perspective on the usefulness of the measure.

4.4.2 Guidelines

This issue can require an in-depth search for cases or situations that show similarities with the situation in which the measure will be implemented. One should not expect that quantitative indications of effectiveness of measures is easily acquired. If no information is available, this still may be worthwhile to note, since it may lead to additional activities to understand the effectiveness of the measure.

Collecting evidence on the effectiveness of a measure could be a time and resource consuming challenge. It also could show to be difficult to get available information in the open. Competitive or political interests might hinder making information available to third parties.

It thus very much depends on the context in which the DSS is used whether one is able or not to spend the needed resources, whether time constraints enable a thorough search or not, and whether political or competitive problems can be overcome.

The questions posed in the table hereunder are aimed at aggregating available evidence on effectiveness and indicating what information is lacking.

4.4.3 Action

Answer the following questions, and record the answers.

Question	
What is known about the effectiveness of the proposed measures?	1. Is any information available that proves the effectiveness of the measure? If so, could you document the information available, and present the main conclusions on evidence of effectiveness? 2. Which attributes are used and/or needed to score the effectiveness of a measure? 3. Are these attributes disputed or contested? If so, on what grounds? 4. Are similar situations known in which similar measures have been inserted/applied? 5. Is information about the effectiveness of these measures in these situations available? If so, could you document the information available and present the main conclusions on evidence of effectiveness in these situations? 6. Do you consider information on the effectiveness of the measure so crucial that additional activities to investigate this effectiveness need to be undertaken? 7. If so, what kind of activities should be undertaken (interviews, focus groups, desk research, empirical investigations, attempts for technical redesign, ….)? Please, explain your choice.

Table 4: Effectiveness of measures proposed

Template used in:					
Self-Directed	Yes	Exploratory	Yes, but depending on context	Comprehensive	Yes

4.5 ALTERNATIVES TO PROPOSED MEASURES

4.5.1 Rationale

Depending on the situation, the set of measures which have been proposed may be limited. It is possible to become fixated upon a particular measure in response to a threat, perhaps because such a measure is new, offers some particular advantage, or is easily available to the responding organisation. This may be the consequence of the perspective of the actor that is responsible for countering the security threat. It may as well be the situation that insufficient attention has been devoted to the kind of measures that could achieve similar results but with less privacy infringements. Without examining the privacy consequences of a measure in depth, it still may be possible to indicate specific measures that seem to score better, for instance because they do not invoke collection and use of personal data. It thus could be useful to challenge the existing set of measures and to brainstorm or discuss whether alternative measures should be inserted in the assessment phase. These alternative measures could score better on the subsidiarity test (are other measures available that can do the job that are less privacy intrusive?) and/or on the proportionality test (is the privacy infringement proportional to the intended goals to be achieved?). It could be that no such alternative measures can be found, but the search process can offer some interesting and novel options that otherwise would have been neglected.

4.5.2 Guidelines

This part of the preparatory phase is an explorative one. Several methods can be used to check whether interesting alternatives are available which are not on the list. One typical approach is the brainstorming session in which a group of people brainstorm on potential approaches, from a range of perspectives. Not only experts could be included in the brainstorm but affected persons could be involved as well. These (directly or indirectly) affected persons may contribute with perspectives that are outside the scope of the experts. Solutions could be sought in terms of radically different ones, using different technologies, using organisational measures, using socio-political measures, instead of relying on e.g. specific technological solutions. Other approaches could use survey results on how people experience specific security solutions, on interviewing interested and involved persons/organisations and on desk research into similar cases.

Depending on the context of the overall assessment (initiated by public authorities, civic organisations or security investors, or enforced through specific forms of legislation and regulation, or part of other initiatives) the chances of getting rich and interesting alternatives will be better or worse. If it shows that alternatives cannot be pursued, the search for alternatives could be postponed until the mitigation phase. This phase also offers some opportunities to insert alternative pathways.

If alternative measures are found to be interesting to use in the assessment phase, these measures should also be checked on evidence re. their evidence. This implies that for these measures the previous section should be repeated.

4.5.3 Action

First, check whether alternatives are available (see template).If not sufficient or in need of a broader range of alternatives, think of ways to open up these alternatives (focus group meeting, survey, interviews, expert consultation). Execute this alternative and inventory the results.

Answer the following questions, and record the answers.

Question	
Are you aware of alternative measures that may achieve similar security goals but that are less privacy invasive?	1. Do you know of any measure that is based on less privacy invasive technologies that could do the job (for instance technology that is based on less privacy invasive principles, such as not collecting personal data)? 2. Do you know of any measure that uses a different approach to achieve the security goals (for instance organisational measures instead of technological measures; or socio-political measures instead of technological or organisational measures)? Please, explain your choice.
Alternative approaches	If time and resources are available, you might consider using explorative methods (focus groups, expert consultation, interviews) to acquire additional input on potential measures. These methods can be focused on security/privacy experts but it might be interested to involve citizens and NGOs as well. They may offer additional perspectives not easily acquired through expert consultations.

Table 5: Alternative measures

At the end of this stage we should be able to create a list of the initial measure and the alternative measures that are to be put through the assessment phase together. One alternative measure that should be considered is doing nothing – although there are often various pressures to take action in a particular context, doing nothing is included as a benchmark against which other options can be evaluated. Please, complete the list of measures to be put through the assessment phase

	Basic security dimensions	Basic privacy dimensions
Initial measure (Measure 1)		
Alternative measure (Measure 2)		
Alternative measure (Measure 3)		

Table 6: List of measures that will be assessed

Template used in:					
Self-Directed	Yes	Exploratory	Yes, but depending on context	Comprehensive	Yes

4.6 AVAILABLE EVIDENCE ON ATTITUDES, PERSPECTIVES AND BEHAVIOUR RELATED TO SECURITY MEASURES

4.6.1 Rationale

Previous parts of the preparatory phase made reference to available evidence to support claims on effectiveness of security measures and alternative options that could do the job with lesser privacy infringements. In addition to these sorts of evidence, information on attitudes, perspectives and behaviour related to security measures will be collected. This information helps in assessing how people will experience specific security measures, how they assess the privacy and broader ethical implications of the measures in relation to the threat and whether alternative measures or approaches will meet preferences of people better. Available evidence can be collected from the various surveys that have been held in recent years throughout Europe on issues of privacy and security (especially the PRISMS and PACT surveys, and the evidence collected from the SurPRISE citizen summits), complemented by country specific surveys. A repository of survey material can be built up over time to help searching for appropriate evidence. Experiences of people as these come forward from case study material (for instance the in depth exploration of security experiences at the Zaventem airport, as studied within PRISMS[1]) forms an additional source of information to be explored.

4.6.2 Guidelines

Depending on the scope and size of the planned security measures, exploring additional evidence on attitudes, perspectives and behaviour of people in specific circumstances will be more extensive or relatively modest. Survey material will be made available that is organised such that it offers direct access to some issues on behaviour and perspectives, but overall one should expect that material usually needs to be ordered and explored on the basis of specific questions. The exercise of examining the available evidence to see if it contains relevant insights for the particular context is itself a useful exercise for a decision maker. The PRISMS and PACT surveys should offer a first help, PRISMS exploring in depth eight typical situations and PACT exploring three typical surveillance technologies. Other surveys, such as the information collected through the SurPRISE focus group meetings and the Eurobarometer survey on privacy attitudes and country specific surveys, can be added to this material.

An additional caveat is in place here. Though the idea of an evidence base is tempting, and PRISMS, SurPRISE and PACT no doubt have collected a load on interesting evidence concerning citizen's attitudes and perceptions, no single project will have the opportunity to structure this evidence such that it can be used in a push button modus. This means that – if resources allow this – the selection and processing of relevant evidence needs to be done by a team of researchers that is involved in the specific challenge. Depending on the setting of the sue of the DSS, collecting and processing available empirical evidence will be part of the work done or left out.

[1] Christiaens, Jenneke, Francesa Menichelli & Serge Gutwirth, Deliverable 4.2 - Final Criminological Report: To Fly or Not to fly - imposing and undergoing airport security screening beyond the security-privacy trade off, 1 April 2015, http://prismsproject.eu/wp-content/uploads/2012/04/PRISMS-D4-2.pdf,

4.6.3 Action

Answer the following questions, and record the answers.

Question	
Are you aware of available empirical material that presents (statistical or case study) evidence on how people experience specific security measures?	1. Please, check available information of the PRISMS survey (presenting behaviour and attitudes in eight different contexts). Please, document relevant findings of this check. 2. Please, check available information of the PACT survey (presenting experiences with three typical security technologies). Please, document relevant findings of this check 3. Please, check available information of the SurPRISe focus groups (discussing three typical security situations with interested citizens). Please, document relevant findings on this check. 4. Are you aware of any other surveys (country wise; topic wise), studies, pilots, cases or other relevant research material that is relevant for the security threat you are exploring?

Table 7: Available evidence on attitudes and perceptions

5 ASSESSMENT PHASE

In the assessment phase we conduct a privacy-focused impact assessment on the proposed security measure and the generated alternative security measures.

A privacy-focused impact assessment is important because it allows for a check against key criteria which justify and legitimate security measures. It helps as well in identifying areas where there are potentially unwanted impacts and externalities.

A key element of the PRISMS impact assessment is that it is a comparative assessment, it assesses a number of measures at once. This allows for comparison between multiple options on a number of variables. By mapping these variables, a decision can be supported which takes into account the respective strengths and weaknesses of the assessed security measures as well as allowing a consideration of their relative proportionality.

The assessment phase contains four elements:

1. The fundamental conditions for privacy
2. Potential infringements of privacy
3. Potential infringements of the right to the protection of personal data
4. Individual, group and categorical impacts and experiences
5. Additional requirements
6. Summarising the impacts

These elements are brought together to compare impacts across different solutions.

Red flags – The PRISMS DSS uses Red Flags to highlight areas which can be particularly troubling for privacy impacts. If an answer to a particular question or exercise might raise a red flag this is noted next to the question. In the mitigation phase (see next chapter) attention will be paid to opportunities to counter the issues which have been signalled with red flags.

Warning signs - In addition to red flags, the DSS also uses Warning Signs to identify areas where they may be privacy and fundamental rights concerns than fall short of presenting a legal barrier or show stopper. Warning signs can also be addressed in the mitigation phase.

Template used in:					
Self-Directed	Yes	Exploratory	Yes	Comprehensive	Yes

5.1 THE FUNDAMENTAL CONDITIONS FOR PRIVACY

5.1.1 Rationale

Security systems must comply with the law. The DSS cannot, however, guarantee by itself compliance with the law. This is also not its objective. On the contrary, the DSS must be seen as an important step in a process of pursuing compliance, notably regarding the crucial issue of compliance with fundamental rights requirements.

Some of the prior building blocks of the DSS have already touched upon important issues to be taken into account from this perspective. The purpose of this building block is to go deeper into some pending questions that are key to understand whether the measure being discussed is compatible with fundamental rights obligations.

In this building block we make a distinction between the fundamental right to respect for privacy and the fundamental right to respect for personal data protection. Both rights are relevant for PRISMS. They refer to different laws and regulations. This leads to a two-steps inquiry whereby firstly we will ask whether the measure encroaches upon the rights to respect for private life and personal data protection, and, if that is the case, secondly we will investigate whether the encroachment can be regarded as lawful.

5.1.2 Existence of an interference with the rights to privacy or personal data protection

The first issue to be addressed is whether the measure constitutes a limitation of the right to respect for private life and/or a limitation of the right to personal data protection. These two rights can in some cases appear to overlap. If so, it is more appropriate to start with addressing the limitation of the right to personal data protection. In order to know whether such a situation (of overlapping rights) is at hand it is best to first consider the question of whether the measure affects the right to the protection of personal data.

To establish the existence of an interference with the right to privacy, it does not matter whether the persons concerned have been inconvenienced in any way. Compliance is always at stake when interference exits, no matter the practicalities of the interference.

A measure might be regarded as actually including different measures which each constitute one or more limitations upon the rights to respect for private life and personal data protection. For instance, generally storing communications data of all individuals in a country and allowing access to law enforcement authorities to stored data related to some persons can be envisioned as encompassing two different measures (one imposing general retention of data, and the other granting access to some data) that affect both the rights to privacy and to personal data protection. In this particular situation, it is thus necessary to address both measures as measures that might potentially interfere with the right to privacy and/or the right to the protection of personal data.

	Issues	Measure 1	Measure 2	---
Does the measure represent a limitation of the right to respect for private life?	Does the measure affect anybody's right to respect for his or her private and family life, home and correspondence?			
	If unclear, please note that: - the right to the respect for private life must be understood as a broad notion.			

Table 8: Existence of a limitation

5.1.3 Assessing the lawfulness of the interference

If a measure constitutes a limitation of the rights to respect for private life or to the protection of personal data, then it is necessary to assess whether the limitation can be regarded as lawful.

To be legitimate, limitations of fundamental rights must:

- pursue a legitimate aim;
- have a legal basis;
- be suitable to pursue the targeted aim;
- be necessary and limited to what is necessary;
- be accompanied by measures ensuring they are limited to what is necessary.

We will present each of these hereunder.

Legitimate aim

Limitations on the exercise of fundamental rights are only permissible if they pursue an objective of general interest, or are justified by the need to protect the rights and freedoms of others.

Objectives of general interest encompass ensuring public security, but are wider. Examples are the fight against international terrorism to maintain international peace and security, fighting against serious crime, or increasing the transparency of the use of public funds.

Legal basis

It is not enough that the measure ultimately pursues a legitimate objective. It must also have a legal ground, that is, there must be a law in place that allows individuals to foresee the existence of such a measure. For instance, if an hospital dealing with patients suspected of being infected with the Ebola virus decides to install CCTV cameras to constantly and systemically record such patients and those who treat them, it must first make sure that there is a law that could allow such practice.[2]

Suitability of the measure

Measures are not permissible if they are not appropriate to attain the objective that they allegedly pursue. They must genuinely meet the objectives they pursue.

[2]Example taken from Martínez, Ricard (2014), *Videovigilancia de enfermos con ébola*, LOPD y Seguridad, http://lopdyseguridad.es/videovigilancia-de-enfermos-con-ebola/.

However, this does not mean that the measure adopted shall be fully reliable. It is enough that the measure significantly contributes to attaining the objective.

Necessity (and limitation of the measure to what is necessary)

Measures that encroach upon fundamental rights should not go beyond what is necessary to attain the objective pursued.

The fact that the pursued objective might be of the utmost importance does not justify, in itself, the necessity of all measures pursuing it.

The assessment of the necessity of the measure also requires to inquire whether the measure corresponds to a pressing social need: it is not enough that somebody believes it could be useful.

The assessment of the necessity of the measure also obliges to ask whether there are alternatives that might allow to pursue the same objective but in a less restrictive manner. This means that for a measure to be regarded as 'necessary' there must be no measure available that is less restrictive but still adequate to attain the objective pursued.

Alternative measures that may be used to achieve similar security objectives as the one intended, have been inventoried in the preparatory phase. In this stage, the measures can be compared.

Ensuring that the measure will not go beyond what is necessary

To make sure that measures that constitute encroachments upon fundamental rights do not go beyond what is necessary to achieve the pursued aim, they must be accompanied by specific safeguards.

Measures shall be governed by objective criteria that make sure that they are limited to what is strictly necessary. This might require establishing distinctions or limitations depending on who is affected.

When a measure involves the processing of personal data, this entails the need to ensure that personal data protection rules are implemented.

When a measure involves the processing of personal data to reduce threats to public security, the data processed must relate to individuals who have a relationship to threats to public security.

	Issues	Measure 1	Measure 2	___
Legitimate aim				
Does the measure pursue an objective of general interest,	No to both = 🚩			
Or is it justified by the need to protect the rights and freedoms of others?	No to both = 🚩			
Legal basis				
Is there a law that allows to foresee the measure?	No = 🚩			

	Issues	Measure 1	Measure 2	___
Suitability				
Is the measure suitable to pursue the targeted objective?	No = 			
Necessity				
Is there a pressing social need for the measure?	Is the measure more than just seemingly convenient? No = 			
Is the measure genuinely necessary to achieve the objective pursued?	No =  Is there another measure that would be just as effective but less intrusive? In order words, is it possible to envisage measures that would interfere less with fundamental rights but still effectively contribute to the objective pursued? Yes =  **If yes, the alternative measure should be privileged.**			
Are there precise rules governing the extent of the interference with fundamental rights?	Are there objective criteria that allow to ensure that the interference only affects those who must be affected, and in the most limited way possible? No = 			

Table 9: Addressing the lawfulness of the interference

Template used in:					
Self-Directed	Yes	Exploratory	Yes	Comprehensive	Yes

5.2 POTENTIAL INFRINGEMENTS OF PRIVACY

5.2.1 Rationale

Privacy is a complex and multi-faceted feature of social life. Privacy can be impacted by security measures in a range of ways. Existing research has started to understand the ways in which privacy can be negatively impacted by security measures. In a complex world it is difficult and potentially impossible to predict what impact a security measure will have in the future. However, based upon previous experience some inferences can be made, and some potential impacts anticipated.

Breaking the impact of security measures on privacy down into a number of dimensions allows us to compare security measures against each other in a more nuanced way, as well as helping us to identify the particular elements of security measures which are likely to cause privacy problems. We may find, in a later stage, that these elements can be removed, or minimised.

The privacy dimensions approach is a way to compare several measures across a number of privacy relevant dimensions. This allows the decision maker to identify those measures which are least privacy invasive. This part of the assessment will be followed by another stage in which the question of privacy is addressed from the perspective of fundamental rights.

5.2.2 Guidelines

The table in this section can be used for comparative purposes between the different measures, but can also raise red flags which shall be addressed by mitigation methods in a later stage. The questions serve to raise the profile of privacy issues which might otherwise be overlooked. The questions are presented in two levels of detail. We recommend completing the top-level questions, and the secondary questions if possible and appropriate. In each case the respondent should provide additional detail where available.

5.2.3 Action

Answer the following questions for each of the measures with a yes or no, and additional detail if possible. Yes answers may be considered to raise warning signs)

Types of privacy	Question	Measure 1	Measure 2	---
Of the person	**Does the security measure impact upon privacy of the person?**			
	Does the security measure involve a search or monitoring of a person's body?			
	Does the security measure involve taking a bodily fluid without consent?			
	Does the security measure involve requirements to submit to biometric measurement?			

Types of privacy	Question	Measure 1	Measure 2	---
Of personal behaviour	**Does the security measure impact upon privacy of personal behaviour?**			
	Does the security measure involve monitoring a person's behaviour?			
	Does the security measure involve recording a person's speech?			
Of personal communications	**Does the security measure impact upon the privacy of personal communications?**			
	Does the security involve intercepting a person's telephone calls or text messages?			
	Does the security measure involve access to a person's email or other communications?			
Of location and space	**Does the security measure impact upon the privacy of location and space?**			
	Does the security measure involve tracking a person wherever he/she goes?			
	Does the security measure involve tracking an individual across websites?			
	Does the security measure involve tracking that allows for a picture of an individual's movements to be constructed?			
Of association and groups	**Does the security measure impact upon privacy of association and groups?**			
	Does the security measure involve processing information on groups of people?			
	Does the security measure involve tracking of associations and/or groups of individuals?			
	Do group characteristics play a role in determining whether tracking occurs or not?			
	Do these groups match recognised social groups?			
	Can the categories be regarded as discriminatory?			

Types of privacy	Question	Measure 1	Measure 2	---
	Are the groups and the way they are created made transparent and available to these individuals and groups?			
Of organisations	**Does the security measure impact upon the privacy of organisations?**			
	Does the security measure involve tracking of organisations?			
	Are the structure or internal secrets of organizations revealed through surveillance?			
	Is the security measure likely to impact upon the functioning of an external organisation or its ability to meet its aims because of any such surveillance or tracking?			
Anonymity	**Does the security measure impact upon anonymity?**			
	Does the security measure aim at lifting anonymity of individuals?			
	Does the system collect or process information on someone who would not have had their information collected or processed before?			
	Does the security measure preserve anonymity of individuals? [Yes answer does not raise a red flag]			
	Through the use of anonymous data, does the security measure have consequences for individuals or groups who would not qualify as data subjects?			
The right to be let alone	**Does the security measure impact upon the right to be let alone of individuals?**			
	Does the security measure impact upon the right to be let alone of associations and/or groups of individuals?			
	Does the security measure include surveillance of areas which would have previously been the sole domain on an individual?			
Right to freedom of expression and communication	**Does the security measure impact upon the right to freedom of expression and communication?**			

Types of privacy	Question	Measure 1	Measure 2	---
	Does the security measure impact upon the right to freedom of expression and communication of individuals?			
	Does the security measure impact upon the ability of groups or individuals to receive information?			
	Does the security measure impact upon the right to freedom of expression and communication of associations and/or groups of individuals?			
	Does the security measure impact upon the freedom of the media?			
	Are any individuals' communications monitored?			
Right to free development of individual and identity	**Does the security measure impact upon the right to the free development of an individual?**			
	Does the security measure impact upon the right to the free development of an individual identity?			
Right to freedom of thought and religion	**Does the security measure impact upon the right to freedom of thought and religion?**			
	Does the security measure impact upon the right to freedom of thought and religion of an individual?			
	Does the security measure impact upon the right to freedom of thought and religion of an association or group of individuals?			
	Does the security measure seek to reveal individuals' thoughts, beliefs or religious identities?			

Table 10: Types of privacy

Template used in:					
Self-Directed	Yes	Exploratory	Yes	Comprehensive	Yes

5.3 POTENTIAL INFRINGEMENTS OF THE RIGHT TO PROTECTION OF PERSONAL DATA

5.3.1 Rationale

The European Charter of Fundamental Rights declares the protection of personal data to be a fundamental right (Article 8). This right refers to the collection, storage, use, dissemination and processing of personal data not being excessive, being related to a specific purpose and being embedded with a number of particular safeguards (concerning the quality of data, the appropriate technical and organisational measures to safeguard the data, and the rights of data subjects). Given the increasing digitisation of security technologies, the emergence of interconnected networks and the abundant availability of data through platforms, smart devices, networks, and information systems, one should expect that introduction of security measures will lead to an increased collection, storage etc. of personal data. The European directive on personal data (95/46/EC)[3] is the main source for identifying what are requirements in dealing with personal data. It is complemented with several other directives and regulations, that may relate to specific approaches (computer criminality, telecom networks provisions, eCommerce, police registers).

5.3.2 Guidelines

In assessing the impact of using personal data in the security measure, the guidelines as proposed by the EU directive on personal data (95/46/EC) are considered. They lead to a number of issues that need to be guaranteed when dealing with personal data.

5.3.3 Action

Please answer the following questions

	Issues	Measure 1	Measure 2	---
Does the measure represent a limitation of the right to personal data protection?	Does the measure involve the processing of personal data?			
	If unclear, please note that; - personal data is any data (text, images, sound recordings, etc.) that relates to somebody who can be identified; for instance, fingerprints constitute personal data.			

Table 11: Data collection and use issues

[3] To be replaced by the EU General Data Protection Regulation in due time.

If the answer to the question is yes, then please complete the second table, which structures the examination of issues related to data collection and use. Again please provide further detail for any "yes" answers, as these may raise warning signs .

Issues concerning data collection and use	Measure 1	Measure 2	---
Are the individuals affected by the security measure identifiable?			
Does the security measure involve the collection of sensitive data?			
Does the security measure involve collection and processing of data on vulnerable subjects?			
Does the security measure enable consent of individuals for collecting and processing personal data? *[Yes answer does not raise a warning sign]*			
Does the security measure allow subjected individuals to exercise their rights to deletion/erasure of personal data (No answer raises a warning sign)			
Are third parties involved in any part of the data collection and processing as part of the security measure?			
What number of persons are affected by the security measure?			
Are there clear and precise rules governing its scope and application?			
If the measure pursues the fight against crime, is there any evidence suggesting the existence of a link between the individuals whose data are processed and crime?			
Does the security measure establish procedures and supervision on the retention of data stored?*[Yes answer does not raise a warning sign]*			
Can affected individuals inform themselves on the specifics of the security measure? *[Yes answer does not raise a warning sign]*			
Will information on the specifics of the security measure be openly and actively communicated to affected individuals? *[Yes answer does not raise a warning sign]*			

Table 12: Data collection and use issues

Template used in:					
Self-Directed	Yes	Exploratory	Yes, but dependent on the context	Comprehensive	Yes

5.5 ADDITIONAL REQUIREMENTS

5.5.1 Rationale

There are likely to be context dependent requirements that we can't anticipate in a DSS. Users can insert their own requirements and evaluate the measures against these. For instance, when security measures are imposed in a working environment, specific legislation of importance to the working situation may need to be met as well. The intent of this section is to check whether such alternative issues play a role. Given the scope of the DSS, it is primarily issues conflicting with or arising in respect to privacy and personal data that we are interested in.

5.5.2 Guidelines

No general rules can be provided here. Much depends on the context of the issue, and the expertise with the legal frameworks that apply to this situation. Depending on the scale and scope of the full exercise, checking for additional requirements can be a relatively fast exercise or a more in depth exploration of domain and context specific additional requirements.

5.5.3 Action

Question: Are there other requirements that the proposed security measure needs to comply with? If so, please detail these here, then evaluate the extent to which the security measures bei*ng analysed meet these requirements (0-4 scale)*

Additional requirement (please detail here)	Measure 1	Measure 2	Measure 3	Measure 4
Additional requirement 1				
Additional requirement 2				
Additional requirement 3				

Table13: Additional requirements

5.5.4 Resources

- Relevant law
- Standards
- Internal requirements and policies

The following table presents some European legislation which may have an impact upon security measure and systems. This should be considered a starting point and not as a comprehensive list. National legislation should be taken into account as relevant.

Way of life, fears and aspirations	Charter of Fundamental Rights of the European Union; European Convention on human rights**;** Council Directive 2000/78/EC of 27 November 2000 establishing a general framework for equal treatment in employment and occupation; Directive 2004/38/EC on the right to move and freely reside; Gender recast Directive 2006/54/EC; Employment equality Directive 2000/78/EC/
Culture and community	Charter of Fundamental Rights of the European Union; Council of the European Union, Directive 2000/43/EC of 29 June 2000 implementing the principle of equal treatment between persons irrespective of the racial or ethnic origin; Racial equality Directive 2000/43/EC
Political systems	Charter of Fundamental Rights of the European Union; European Convention on human rights.
Environment	Directive 2008/1/EC of the European Parliament and the Council of 15 January 2008 concerning integrated pollution prevention and control: Directive 2011/92/EU of the European Parliament and the Council of 13 December 2011 on the assessment of the effects of certain public and private projects on the environment.
Health and well-being	National Legislation for health; Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare; Council Directive of 12 June 1989 on the introduction of measures to encourage improvements in the safety and health of workers at work (89/391/EEC).
Personal and property rights	Charter of Fundamental Rights of the European Union; Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data; Directive 2002/58/EC of the European Parliament and the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector; Employment Equality Directive 2000/78/EC; Gender goods and services Directive 2004/38/EC; Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.

Table 14:Regulatory and legislative sources4

[4]Wadhwa, Barnard-Wills & Wright, 2014, http://spp.oxfordjournals.org/content/early/2014/08/25/scipol.scu046.abstract

Template used in:					
Self-Directed	No	Exploratory	Yes, but dependent on the context	Comprehensive	Yes

5.6 INDIVIDUAL, GROUP AND CATEGORICAL IMPACTS AND EXPERIENCES

5.6.1 Rationale

Privacy and data protection law (and related laws with an impact on privacy and/or data protection) do not include all the ways in which a security measure might have unwanted impacts. People may for instance experience security measures as illegitimate and unjustified, as measures that have disproportionate consequences for specific groups of people. People may also experience the impact of security measures, being indirectly affected individuals, and may feel disproportionately affected by these measures. An example of this latter situation is the shielding off of a region of a city when some high-level event occurs (such as the visit of a high profile guest, or the organisation of a Summit in a city). The way that individuals and groups experience security measures may heavily influence the effectiveness of a measure. The more people experience security measures as justified, legitimate and serving their interests, the more the security measures will be accepted as relevant and contributing to safety, security, health and happiness of individuals and society at large. Concerns voiced by directly and indirectly affected individuals and groups of people may refer to a broader range of ethical concerns, broader than concerns on privacy and personal data. They deal with feelings of unrightfully being discriminated against, being excluded in inappropriate manners and the like. Security measures can be negatively experienced even if they are legally compliant. Similarly, even if a measure is accepted by the public, it may still violate fundamental rights, or may not be compliant with appropriate law. This type of impact is particularly important for how the security measure is received, and for how people are likely to respond to it.

In identifying these sorts of impact, so-called ‘rebound’ effects will be identified as well as so-called ‘systemic’ effects. ‘Rebound’ effects are consequences of a measure that negatively affect the effectiveness of that measure. An example of a ‘rebound’ effect of installing CCTV to fight drugs criminality is that the criminality will transfer to another neighbourhood, causing similar problems in this neighbourhood. A ‘systemic’ effect could be that in the end all neighbourhoods will have CCTV with potential negative consequences for feelings of security in these regions.

The aim here is not to “market” the security measure, but rather to identify, based upon available and gathered evidence, the ways in which security measures such as those proposed are experienced by individuals and groups, in a role of being directly affected by the security measures and of being indirectly affected. It also acts as another way to compare different security measures.

Practically, this step may include some additional research to understand the experiences and perspectives in relation to the particular security measures proposed and in the particular context of their use.

5.6.2 Action

Please answer the following questions:

	Issues	Measure 1	Measure 2	---
Issues concerning experiences of **directly affected** individuals and groups of people with security measures	Are the security measures experienced by individuals as being disrespectful? (yes = )			
	Are the security measures experienced by individuals/groups of people as being discriminatory? (yes = )			
	Are the security measures experienced by individuals/groups of people as being dehumanizing? (yes = )			
	Are the security measures experienced by individuals/groups of people as being stigmatizing? (yes = )			
	Are the security measures experienced by individuals/groups of people as having a disproportionate impact on daily life? (yes = )			
	Are the security measures experienced by individuals/groups of people as having a disproportionate impact on quality of life (social, economic, health)? (yes = )			
	Is the security measure experienced by individuals/groups as creating or exacerbate a power imbalance ? (yes = )			
Issues concerning experiences of	Are the security measures experienced by individuals as being disrespectful?			

	Issues	Measure 1	Measure 2	---
indirectly affected individuals with security measures	(yes = )			
	Are the security measures experienced by individuals as being discriminatory? (yes = )			
	Are the security measures experienced by individuals as being dehumanizing? (yes = )			
	Are the security measures experienced by individuals as being stigmatizing? (yes = )			
	Are the security measures experienced by individuals as having a disproportionate impact on daily life? (yes = )			
	Are the security measures experienced by individuals as having a disproportionate impact on quality of life (social, economic, health)? (yes = )			
	…			

Table 15: Individual impacts and experiences

	Issues	Measure 1	Measure 2	---
Issues concerning opportunities to deal with the impact of security measures	Do directly affected individuals/groups of people perceive opportunities to 'deal with' the imposed security measures?			
	Do indirectly affected individuals perceive opportunities to 'deal with' the imposed security measures?			
	Can directly affected individuals/groups of people			

	Issues	Measure 1	Measure 2	---
	organise counter measures against the imposed security measures?			
	If Yes, are the counter measures negatively affecting the effectiveness of the security measures?			
	Do indirectly affected individuals organise counter measures against the imposed security measures?			
	If Yes, are the counter measures negatively affecting the effectiveness of the security measures?			
	Can any longer term implications of security measures be identified that may negatively affect the impact of the security measures?			

Table 16: Counter measures by individuals

5.6.3 Resources

- Some **statistical data** on European citizen's perspectives on security measures is available through the PRISMS survey, as well as the findings of the PACT and SuRPRISE projects.
- **Literature** on how people experience security measures affecting their daily life.[5]
- **Case studies** on the adoption of similar types of technologies in related contexts can provide information on how people reacted and responded to those technologies.
- **Interviews and focus groups** can be conduct with people and groups that are likely to be subject to the security measure. They may have access to insights and perspectives that the security decision maker may not have, and may be able to advise on how the security measures might impact upon them.

[5] See for instance: Frey, Bruno S., Lüchinger Simon, and Alois Stutzer, "Valuing Public Goods – A Life Satisfaction Approach", CESifo Working Paper 1158, CESifo GmbH, Munich, 2004. https://www.cesifo-group.de/DocDL/cesifo1_wp1158.pdf

Template used in:					
Self-Directed	Yes	Exploratory	Yes	Comprehensive	Yes

5.7 SUMMARISING THE IMPACTS

This final part of the assessment phase brings together the evidence that has been put together in this section into a comparable form that can be used to aid decision-making.

5.7.1 Rationale

Having performed the assessment on security measures proposed and added from a variety of perspectives, the next stage is to synthesize the main findings, in order to create a better understanding on the impacts of the security measures. Synthesizing helps in identifying so-called 'red flags', i.e. signposts indicating troublesome features of the security measures which may seriously hamper the use and acceptance of these measures. It also helps in identifying opportunities to improve privacy respecting features of the security measures, by inserting additional organisational and technical measures that help preventing privacy infringements *a priori*(privacy by design). Finally, it may help in understanding ethical concerns of directly and indirectly affected individuals, concerns that as well could be legitimate (because of illegitimacy of security measures) as not necessarily legitimate but clearly grounded in social and individual concerns relating to daily life and quality of life issues.

5.7.2 Guidelines

In order to somewhat 'quantify' the impacts, the information collected in the previous stages is grouped together in the following table into categories under one of a number of headings. The answers to these categories can be given a rating between 0 and 3 (for example 3 = serious impact, 2 = high impact, 1 = low impact, and 0 = no impact) so that this summary table can then be used to generate radar-plots for the various assessed measures.). This collation is done to ease comparative understanding of the various security measures, and not in order to pass a definitive judgment on the assessed security measures. The previous answers to the more specific questions still remain relevant. The scoring only servers a heuristic objective, in that it offers an easy to check visualisation of the various measures!

 Answers at the level of "serious impact" or "high impact" are red flags. Please note that these red flags likely represent a number of individual issues raised in the component sections. A number of warning signs in a single area may collectively represent a red flag

5.7.3 Action

The synthesis will be guided by the following set of questions:

	Issues	Measure 1	Measure 2	---
Legitimacy of the security measures	In what sense are the security measures legitimate? In what sense are they based on a legal basis? In what sense are they suitable? In what sense are they necessary? In what sense do they limit themselves to what is strictly necessary?			

	Issues	Measure 1	Measure 2	---
	[see Tables 9]			
Privacy dimensions	What impact do the security measures have on the respective privacy dimensions (privacy of the person, privacy of behaviour, privacy of communications, privacy of location and space, privacy of association and groups, privacy of organisations) (serious impact – high impact – low impact – no impact)? [see Table 10]			
Rights and Freedoms	What impact do the security measures have on the respective rights (right to be left alone, right to freedom of expression and communication, right to freedom of development of individual identity, right to freedom of though and action)? (serious impact – high impact – low impact – no impact) [see Table 8]			
Data protection dimensions (1)	What impact do the security measures have on the respective DP-dimensions (identifiable persons, sensitive data, vulnerable groups, consent, number of affected persons) (serious impact – high impact – low impact – no impact) [see Table 11 & 12]			
Ethical concerns	What impact do the security measures have on the ethical concerns of directly affected individuals and groups of people (being treated disrespectful, being discriminated, being dehumanized, being stigmatized, impacting on daily life, impacting on quality of life) (serious impact – high impact – low impact – no impact) [see Table 15 & 16]			
	What impact do the security measures have on the ethical concerns of indirectly affected individuals (being treated disrespectful, being discriminated, being dehumanized, being stigmatized, impacting on daily life, impacting on quality of life) (serious impact – high impact – low impact – no impact) [see Table 15 & 16]			
Additional requirements	To what extent do the security measures meet additional requirements? [see Table 13]			

Table 17: Understanding the impact – synthesis table

6 MITIGATION PHASE

One of the functions of the PRISMS DSS is to help to reduce the negative, unintended and unwanted privacy impacts of security solutions that are applied in response to a security problem. Whilst the assessment phase(and particularly the summary of impacts conducted in the previous step) can allow for the selection of those security solutions with the lowest unwanted impact, it is also the case that even the best available option might have impacts that we would prefer to avoid, or have ways in which that impact could be reduced.

In the **mitigation phase** potential additional adjustments are considered which can be added to the security solutions in order to reduce their unwanted impacts. Different security solutions may be more amenable to mitigation measures than others and this can influence the final choice of a security measure.

The mitigation step is therefore a moment of consideration and reflection, following the impact assessment, on ways to reduce the negative impacts and/or side effects of security solutions, in a way which can be helpful and included in the comparison of alternatives in the final decision stages.

The mitigation phase consists of the following steps:

1. Inventory of red flags and possibility of mitigation
2. Can the system be reconfigured to better meet data protection principles?
3. Mitigating long term impacts
4. Summary of mitigation measures

Template used in:					
Self-Directed	Yes	Exploratory	Yes	Comprehensive	Yes

6.1 INVENTORY OF RED FLAGS, WARNING SIGNS AND POSSIBILITY OF MITIGATION

6.1.1 Rationale

Various stages during the impact assessment phase will potentially have raised red flags and warning signs in relation to various potential impacts arising from the assessed security measures. These red flags will be based upon legal considerations, and upon the impacts of security measures. This stage performs an inventory of these red flags. It also prompts the decision maker to separate problematic issues into two categories: 1) those red flags that are so serious that they prevent the implementation of the security measures (at least in its current form), for example if it has been established that a security measure violates a legal requirement. Red flags might also be termed "showstoppers", in that if left unmitigated, they remove the security measure from the pool of candidates. The second category of issues are warning signs, that whilst not showstoppers do raise issues or concerns with regard to the security measure. These might also be responded to through mitigation measures to reduce the unwanted and negative impact of these measure upon the privacy of individuals and groups. This building block checks to see if these red flags and warning signs can be "lowered" again. It starts from a position that these flags and signs are meaningful and should be seriously addressed if the security measure is to be adopted.

This stage also makes an assessment of the possibility of mitigating any of these red flags or warning signs. Some security measures are more flexible than others. The design of a security system may be relatively fixed, however even with fixed systems there are many different ways in which they can be implemented. The way a system or technology is implemented can affect the way that it impacts upon people.

6.1.2 Guidance

This stage draws upon the red flags raised in the preceding phase. Please transpose any red flags and warning signs raised in Tables 5.1-.5.7, then provide a short description of the nature of the issue. Then make an assessment of the severity of the issue (e.g., if it is a showstopper or otherwise). Our starting assumption is that most security measures are open to some form of change or variation in their design, implementation or use, which could act as a way to reduce their unwanted impacts.

It is also possible to remove a security measure from the DSS process at this stage if the decision maker believes that it has accumulated too many serious red flags and that these cannot be mitigated. This is also an opportunity for the decision-making organisation to reflect upon their own ability to exert influence over the considered security measures. A security solution being proposed for the particular security problem may be suitable for other security problems, but less so in the particular context being considered here.

6.1.3 Actions

Please complete the following table. Please provide details of any potential mitigation options.

Section	Nature of the red flag or warning sign	Severity (showstopper or concern)	Mitigation options
Measure 1			
e.g. Fundamental conditions for privacy			
Measure 2			
Measure 3			

Table 17 - Inventory of red flags and mitigation options

Template used in:					
Self-Directed	Yes	Exploratory	No, in general not	Comprehensive	Yes

6.2 CAN THE SYSTEM BE RECONFIGURED TO BETTER MEET DATA PROTECTION PRINCIPLES?

6.2.1 Rationale

In addition to mitigating particular problems raised by the design and implementation of a security measure, it may be possible to improve the privacy impact of a security measure by drawing upon existing best practices in privacy sensitive design. These could be applied even to a security measure that seemed to have very low negative impacts upon privacy to further improve its design. Privacy and data protection laws cannot, and do not encompass all the ways in which security systems measures might impact upon privacy. In addition to removing barriers, privacy sensitive design and other best practices can further reduce the impacts of a measure upon privacy above and beyond legal compliance.

6.2.2 Guidelines

This section of the DSS is loosely structured, because of the potential depth of detail of these approaches, and the need to remain applicable to a breadth of potential security measures. This section therefore provides summaries of existing approaches, pointers towards resources on privacy principles, and invites the decision maker to reflect upon the security measures in the light of these. Resources for this stage, including details of these principles and approach can be found in Annex 6

6.2.3 Action

Fill in the following table:

After consideration of the resources available on privacy principles, are there any ways in which the security measures being assessed might be reconfigured to better align with these principles?
Data protection principles: 1. Collection limitation 2. Data quality 3. Purpose specification 4. Use limitation 5. Security safeguards 6. Participation 7. Accountability Data protection by Design: 1. Privacy by default (opting in/opting out) 2. End user control and choice 3. Life cycle approach to data protection 4. Data retention and destruction

Table18: Applying privacy principles

Template used in:					
Self-Directed	Yes	Exploratory	Yes, but dependent on the context	Comprehensive	Yes

6.3 MITIGATING LONG TERM IMPACTS

6.3.1 Rationale

Security measures can have long term, indirect consequences. For example, consider an example where the installation of CCTV has been used as a security measure in response to the threat of physical crime in an area. The *long term* or *systemic* security effect is that in the end all neighbourhoods will have CCTV, that a full system of CCTV monitoring throughout the city is installed and that the net effect of the CCTV potentially falls back to zero since CCTV is no longer a discriminating factor that can be used as an effective security measure. Meanwhile, the privacy consequences of having CCTVs may have gone up, since requests for ever more stringent security measures are put forward by concerned citizen. Given that they are indirect, occur in the future, and are dependent upon many other situational and contextual variables, these impacts are difficult to predict. However, mitigation measures may potentially offer ways to identify these impacts over time, and take steps to address them.

6.3.2 Guidelines

This is another loosely structured step, offering a moment for the decision maker to reflect upon the longer-term impacts of the analysed security measures.

6.3.3 Action

Answer the following question per security measure.

What might be the longer-term impacts of the security measures, and what mitigation steps might be taken to reduce, identify, or monitor long term and indirect consequences of the security measures?
Measure 1: Measure 2: Measure xxx:

Table 19 - Inventory of red flags and mitigation options

Template used in:					
Self-Directed	Yes	Exploratory	Yes	Comprehensive	Yes

6.4 SUMMARY OF MITIGATION MEASURES

6.4.1 Rationale

This allows for a final comparison of the alternative security measures which includes the ways in which they can be modified. The list of mitigation measures for each security measure can be included into additional requirements for the procurement and installation of that measure if it is adopted. The available mitigation options may change the relative impact upon privacy of the analysed security measures. For example, one measure may have been initially evaluated as having a very serious impact upon privacy, but could be so adaptable and customisable that many of these impacts could easily be mitigated. Another measure may have initially scored moderately well (moderate to low privacy impact) but is so fixed (perhaps because it is an off the shelf solution), with little mitigation options available, that this score cannot be adjusted.

6.4.2 Guidance

This stage pulls together any identification measures identified as necessary or desirable during the mitigation phase. It offers a suitable record for future use during the implementation of any selected security measures, of why mitigation measures were selected and their priority.

6.4.3 Actions

Please complete the following tables. Provide details of any mitigation measures that have been identified in the preceding stages, along with if this measure is necessary or it if is simply a desirable option that may be considered on other grounds. Also note what the intended result of this mitigation measure is.

Measure 1	Mitigation Measures	Necessary or desirable?	Motivation
	Please provide details of any mitigation measures to be added to the security measure		What is this mitigation measure intended to achieve?

Measure 2	Mitigation Measures	Necessary or desirable?	Motivation
	Please provide details of any mitigation measures to be added to the security measure		What is this mitigation measure intended to achieve?

Measure 2	Mitigation Measures	Necessary or desirable?	Motivation
	Please provide details of any mitigation measures to be added to the security measure		What is this mitigation measure intended to achieve?

Table 20 - Mitigation summary

7 REPORTING PHASE

During the various stages of the assessment information will be collected and stored in digital and reproducible form. Part of the templates to be used in various stages will be web-based templates, enabling the delivery of input in digital forms that are automatically stored as part of the DSS.

The scope of the reporting phase is to present in a clear and concise manner the main findings of the assessment and the conclusions to be drawn from this assessment. In the end the reporting phase will produce a report that contains the relevant findings, relevant reflections on these findings, if necessary an elaboration of opinions of specific interest groups (public authorities, public interest groups, security investors) and conclusions with regard to the foreseen investment.

Though the DSS can be used for more generic purposes as well, such as inducing involvement of citizen groups in – foreseen – security and surveillance practices, and as such acting as a tool to support participatory decision making and participatory design approaches, the PRISMS DSS has as its prime focus a – foreseen – security investment that is subsequently submitted to an assessment on its foreseen privacy implications and that subsequently is revisited for potential mitigating measures to assure the least privacy infringements possible (presuming legal constraints are met). The report will reflect this scope, so that the main actor is supported in his/her attempt to arrive at balanced and well-thought decisions concerning how to cope with the presumed threat.

The reporting phase will summarise the main findings of the three previous phases. Before doing this, it will address three aspects that help interpreting the results of the previous phases in a slightly different manner. It will start by highlighting pros and cons of the various measures studied, it will continue with presenting constraints and limits of the various measures and finally it will address the wider societal context of the measures. Finally, all aspects of the assessment will be summarised in a management summary.

In the following the headlines of the various parts are presented.

1. Pros and Cons of the measures
2. Constraints and limits
3. The wider social context
4. Final conclusions

Template used in:					
Self-Directed	Yes	Exploratory	Yes, but dependent on the context	Comprehensive	Yes

7.1 PROS AND CONS OF THE MEASURES

7.1.1 Rationale

Pros and cons will differ depending on the actor interviewed. What could be an advantage for one party could be experienced as an infringement to another party. No reality exists that is experienced similar by all involved. The intention is to elucidate the various positions that can be discerned in the assessment made and to clarify the contingency/flexibility of the interpretation. This helps in identifying those issues that have high priority for one party while other parties might dismiss these priorities as irrelevant or 'coming at a specific cost'. And this in turn helps in the comparative assessment of the various measures assessed.

7.1.2 Guidelines

On the basis of the results of the assessment specific pros and cons will be identified. Since the identification and description of pros and cons will vary between the actors, it starts with the identification of the relevant actor groups. Three dominant groups can be identified:

1. The actor who intends to implement a security measure (security investor)
2. The actor to whom the security measure is primarily oriented
3. The actor who may experience the consequences by the security measure without being the primary 'target' (directly or indirectly affected individual/group/category).

Each of these three actor groups can most likely be subdivided in smaller actor groups. Depending on the scope and scale of the assessment this should be done (for instance subdividing the implementers in those who are politically/organisationally responsible and those who do the real implementation).

For each of the actor groups the most relevant pros and cons of the intended security measures are inventoried. This runs through the two phases which are oriented towards the assessment of the measures: assessment and mitigation phase.

7.1.3 Action

Please, fill in the table underneath. Check per phase which three pros and cons are most outstanding for which actor group.

Pick the actor group	Pick the phase	Measure 1	Measure 2	---
Security investor	*Pros and cons identified in the assessment phase:* What pros and cons can be identified in terms of the legal aspects of the measures? What pros and cons can be identified in terms of the privacy aspects of the measures? What pros and cons can be identified in terms of the data protection aspects of the			

Pick the actor group	Pick the phase	Measure 1	Measure 2	---
	measures? What pros and cons can be identified in terms of citizen concerns of the measures? What pros and cons can be identified in terms of ethical aspects of the measures?			
	Pros and cons identified in the mitigation phase: What pros and cons can be identified in terms of tackling the identified red flags? What pros and cons can be identified in terms of potential mitigation measures to relief the privacy infringements of the measures? What pros and cons can be identified in terms of potential reconfiguration approaches with regard to the measures? What pros and cons can be identified in terms of mitigation of citizen concerns of the measures?			
Target group	*Pros and cons identified in the assessment phase:* What pros and cons can be identified in terms of the legal aspects of the measures? What pros and cons can be identified in terms of the privacy aspects of the measures? What pros and cons can be identified in terms of the data protection aspects of the measures? What pros and cons can be identified in terms of citizen concerns of the measures? What pros and cons can be identified in terms of ethical aspects of the measures?			
	Pros and cons identified in the mitigation phase: What pros and cons can be identified in terms of tackling the identified red flags? What pros and cons can be identified in terms of potential mitigation measures to relief the privacy infringements of the measures?			

Pick the actor group	Pick the phase	Measure 1	Measure 2	---
	What pros and cons can be identified in terms of potential reconfiguration approaches with regard to the measures? What pros and cons can be identified in terms of mitigation of citizen concerns of the measures?			
Affected individuals/ groups/ categories	*Pros and cons identified in the assessment phase:* What pros and cons can be identified in terms of the legal aspects of the measures? What pros and cons can be identified in terms of the privacy aspects of the measures? What pros and cons can be identified in terms of the data protection aspects of the measures? What pros and cons can be identified in terms of citizen concerns of the measures? What pros and cons can be identified in terms of ethical aspects of the measures?			
	Pros and cons identified in the mitigation phase: What pros and cons can be identified in terms of tackling the identified red flags? What pros and cons can be identified in terms of potential mitigation measures to relief the privacy infringements of the measures? What pros and cons can be identified in terms of potential reconfiguration approaches with regard to the measures? What pros and cons can be identified in terms of mitigation of citizen concerns of the measures?			

Table 21: Identification of pros and cons per security measure

Template used in:					
Self-Directed	Yes	Exploratory	Yes, but dependent on the context	Comprehensive	Yes

7.2 CONSTRAINTS AND LIMITS

7.2.1 Rationale

Constraints to the measures proposed can be of various dimensions:

1. Legal constraints
2. Financial constraints
3. Institutional constraints
4. Time constraints

Legal constraints have been identified in the assessment phase. Financial and institutional constraints are more difficult to assess. Identifying financial constraints to specific security investments requires a dedicated approach. This is beyond the scope of this DSS. Institutional constraints can be more easily identified. The lack of cross border cooperation could be such a constraint. Time constraints relate to the availability of time to implement and execute the measures. Reaction times can be brief, for instance when a cyber-attack occurs. The analysis of constraints and limits will be based upon the assessment already made but will add some details to this assessment which might require some additional research (interview, desk research).

7.2.2 Guidelines

While the identification of legal constraints is straightforward (already captured) the identification of the other constraints (financial, institutional, time, other) may require additional investigations. Whether this is feasible depends on the scope and scale of the exercise. If sufficient resources are available, one can investigate at greater depth which financial, institutional and other constraints need to be met. Capital investments, organisational settings, availability of a sufficiently skilled labour force (for instance for enforcement purposes) are issues that can put constraints. They could be identified, and subsequently elaborated if sufficient resources are available.

7.2.3 Action

First, check whether legal constraints have been identified. Then, check whether resources are available for a more in-depth exploration or whether one only can perform a marginal research on constraints.

Use the following table.

Constraint		Measure 1	Measure 2	---
Legal	Did you identify any legal constraints?			
Financial	Are you aware of any financial constraints? If so, are you able to explore the dimensions of this constraint in more			

Constraint		Measure 1	Measure 2	---
	depth? If yes, please do so. Describe the result of the investigation.			
Institutional	Are you aware of any institutional constraints? If so, are you able to explore the dimensions of this constraint in more depth? If yes, please do so. Describe the result of the investigation.			
Time	Are you aware of any time constraints? If so, are you able to explore the dimensions of this constraint in more depth? If yes, please do so. Describe the result of the investigation.			
Other	Are you aware of any other constraints? If so, are you able to explore the dimensions of this constraint in more depth? If yes, please do so. Describe the result of the investigation.			

Table 22: Identification of constraints and limits

Template used in:					
Self-Directed	Yes	Exploratory	Yes, but dependent on the context	Comprehensive	Yes

7.3 THE WIDER SOCIETAL CONTEXT

7.3.1 Rationale

In order to overcome the problem of only looking at direct consequences, this assessment also pays attention to indirect, or rebound, and longer term, or systemic consequences of the measures. Rebound consequences are secondary order effects, that arise because of the implementation of a security measure. An example is the replacement of drugs trafficking from one neighbourhood to the other when the first neighbourhood is confronted with heavy police overview. Similarly, systemic implications could be – to stay with this example – that in the end police overview has not resulted in reducing drugs trafficking but in more and more intense surveillance activities without clear results. While rebound consequences can be 'on the radar', long-term strategic implications are more difficult to predict or identify. Still, it might help having this discussion within the assessment. The direct implications of specific security measures for the wider societal context is the first issue to be tackled.

7.3.2 Guidelines

This exploration starts with the immediately visible wider societal consequences. These already have been addressed in the assessment and mitigation phase. Then the rebound aspects are inventoried, as well as the longer-term systemic consequences.

See section 4.3 and 5.6 (full table) that both address rebound and longer term systemic consequences. Information of these sections can be used to answer the issues posed hereunder.

7.3.3 Action

When addressed in detail in 4.3 and 5.6 this information can be inserted here. If deemed necessary, a more detailed analysis can be inserted. Use the following table.

Scope	Issues to be addressed	Measure 1	Measure 2	---
Direct implications	Are any societal consequences conceivable that directly relate to the intended implementation of the security measure and that relate to privacy or personal data?			
	Are mitigation measures conceivable that mitigate these consequences?			
Rebound consequences	Do indirectly affected individuals organise counter measures against the imposed security measures?			
	If Yes, are the counter measures negatively affecting the effectiveness of the security measures?			
	Are mitigation measures conceivable that mitigate these consequences?			
Longer term systemic consequences	Can any longer term implications of security measures be identified that may negatively affect the impact of the security measures?			
	Are mitigation measures conceivable that mitigate these consequences?			

Table 23: Wider societal context – direct, rebound and systemic implications

7.4 FINAL CONCLUSIONS

7.4.1 Rationale

To support the decision maker and the audience addressed, the overall conclusions of the study will be formulated. This will be similar to what normally is considered to be a management summary, entailing in a very concise and bullet-wise manner the main conclusions of the project.

7.4.2 Guidelines

Discuss the main issues that need to be communicated about the results of the assessments to the decision maker, the contractor, a broader audience or whatever specific group is in view. Use can be made of the summaries made at the end of the assessment phase and the mitigation phase (see Table 17: Understanding the impact – synthesis table).

7.4.3 Action

Use Table 17: Understanding the impact – synthesis table and the results of the preceding sections to draft a management summary capturing the main results of the assessment.

8 ANNEXES

8.1 BRINGING SECURITY AND PRIVACY IN ONE ENCOMPASSING FRAMEWORK

The PRISMS DSS draws upon the research into privacy from the PRISMS project and from other related research. The PRISMS deliverable *D1.1: Central concepts and implementation plan* summarised the extent to which privacy is a contested concept that has been notoriously difficult to pin down. The report identified both negative (taxonomies of privacy infringements) and positive (focused on pro-active approaches that prevent privacy harms rather than providing redress) concepts of privacy. The PRISMS DSS, and in particular its identification of privacy dimensions, draws upon both of the former traditions of thinking about privacy, but is more closely aligned to the latter.

Despite the conceptual complexity of privacy (and of security!), in practice the relationship between privacy and security is commonly understood as a trade-off, where increases in security inevitably curb the privacy enjoyed by the citizenry, and as a converse where providing additional protection or guarantees of privacy would have some negative implications for security. Thus, mainstream literature on the public perception of security technologies generally aims to discover how much privacy citizens are willing to trade in exchange for greater security (there are also other understood trade-offs for example between privacy and economic benefit, or convenience).[6] The trade-off model has, however, been criticized, because it approaches privacy and security in abstract terms, and because it reduces complex public opinion to one specific attitude, in which privacy and security are perceived as mutually exclusive goals that cannot be simultaneously achieved through specific – technical – solutions.[7] The language (and practical application) of the trade-off often takes place in a cultural and organisational context which systematically favours security (security decision makers have explicit responsibilities for security, but less so for privacy), which tends to balance the security of majorities against the privacy of minorities, rarely entails a close consideration of what exactly is being measured and balanced, and can be unduly influenced by the unknowability of future security risks.[8] The systematic recourse to the notion of ‘‘balancing’’ suggests that privacy and security can only be enforced at each other’s expense, while the obvious challenge is inventing a way to enforce both without loss on either side.[9]

The DSS privacy framework draws upon (but is not limited to) European privacy and data protection law, and to that extent is calibrated for use in the European context. However, to the extent that other jurisdictions mirror European approaches to privacy the approach may be transferable. Additionally, given that the aim of the DSS is not to show legal compliance, those elements based upon the European approach to data protection can be understood as an example of good practice. EU law relies currently on a separation between ‘privacy’, on the one hand, and the protection of personal data, on the other, as different legal notions. The relation between them is however not univocal: ‘Privacy’ (to be read here as synonymous to ‘respect for private life’) is for EU law something that EU data protection law was originally substantiating (as illustrated by the reference in Directive 95/46/EC), but that came later to be recognised as a notion different from personal data protection, which acquired with such

[6] A hypothetical and in our view undesirable ‘privacy and security Trade-Off DSS’ might show in what circumstances and by ‘how much’ a trade off could be made.
[7] Marc Van Lieshout, Michael Friedewald, David Wright & Serge Gutwirth, “Reconciling privacy and security”, *Innovation: the European Journal of Social Science Research*, Vol.26, No. 1-2, pp. 119-132, 2013; Charles D. Raab, “Privacy as a Security Value”, pp. 39-58 in Dag Wiese Schartum, Lee Bygrave and Anne Gunn Berge Bekken (eds.), *Jon Bing: EnHyllest / A Tribute*, Oslo: Gyldendal, 2014
[8] Lucia Zedner, 2009, 135-136
[9] Van Lieshout et al, Op cit,

evolution an autonomous status (as proved by the EU Charter of Fundamental Rights). The DSS approach acknowledges that attitudes and cultural norms regarding security and privacy might vary between countries, even within the EU, and therefore adopts a comparative approach between different potential security solutions to an identified problem (a security threat of some form), in a particular localised context.

The DSS privacy framework draws upon approaches in privacy risk management. This acknowledges and seeks to identify the potential harms that can arise from the security systems that infringe upon privacy of individuals and groups, and then attempts to reduce such risks posed by these systems. The PRISMS DSS draws upon on-going work on privacy and surveillance impact assessments (PIA and SIA). Privacy impact assessments are a tool used to identify and reduce the privacy risks of projects. Surveillance impact assessments have been developed as privacy impact assessments do not encompass all the implications of a surveillance project.[10]

In the approach of PRISMS, there is a close relationship between the concepts of privacy and surveillance. Surveillance is not limited to physical watching, but is understood as any process which includes the structured collection and processing of information on individuals or groups for a wide range of managerial and governmental purposes, a sub-section of which are security related. It involves control, influence and management through the medium of information, and is a combination of knowledge and intervention.[11] Surveillance can have a wide range of impacts upon people, impacts that include, but are not limited to violations of individual privacy.

The SAPIENT project[12] worked to establish and analyse impacts posed by future smart surveillance technologies that may be used for profiling citizens in order to identify potential evil-doers, for crime control in urban settings or for border control and critical infrastructure protection. It developed a surveillance impact assessment methodology as part of a privacy and surveillance impact assessment (PSIA). The SAPIENT approach was based upon a series of questionnaires designed to determine the key sources of impacts arising from surveillance-based practices. These questions, and the underlying pathways to impact, were decomposed and used as the main basis for the PRISMS privacy dimensions.

The driving motivation with the privacy and surveillance elements of the PRISMS DSS (in line with the SAPIENT DSS) is to foreground additional risks and harms arising from surveillance and security practices, which are often overlooked, discounted, or externalised in security decision making. The process aims to place these factors and issues on a procedurally equal grounding with the factors typically used by decision makers to assess the worth of a security intervention (cost, speed, efficacy, reliability etc.). The second move of the DSS is to introduce reflexive questions that may not have firm operationalized answers into a decision-making system (for example, one issue raised in the PRISMS DSS and in the SAPIENT approach is related to the dimension of power imbalances) but are intended to introduce a moment of thought on this topic into the process. Thirdly, The PRISMS DSS is also intended to promote the societal dimension of privacy[13] in addition to more traditional

[10]Wright, D. & C.D. Raab, (2012) "Constructing a Surveillance Impact Assessment", *Computer Law and Security Review*, 28. 613-626.
[11] Barnard-Wills, D. (2012) *Surveillance and Identity: Discourse, Subjectivity and the State*, Ashgate, Farnham, p. 2.
[12] See http://www.sapientproject.eu/
[13] Regan, P.M., (1995) *Legislating Privacy: Technology, Social Values and Public Policy*, Chapel Hill, NC: University of North Caroline Press; Gutwirth, S. (2002) *Privacy in the Information Age*, Lanham MD: Rowman & Littlefield; Bennett, C. and C. Raab (2006) *The Governance of Privacy: Policy Instruments in Global*

individualist framing. The cluster of privacy dimensions on social context is the most obvious manifestation of this. Finally, the DSS is intended to help build privacy- protecting measures (and measures that mitigate the harms that can be caused by security and surveillance technologies) into systems at an early stage in the planning process.

8.2 THE CONCEPTS OF PRIVACY AND DATA PROTECTION

As the DSS privacy framework draws upon the legal conceptualisation of security, privacy and personal data protection in EU law, a key component of its design is the distinction between privacy and personal data protection as operationalized in this context.[14]

8.2.1 Privacy

In EU law, the term privacy is used primarily to refer to the right to respect for private life established by Article 8 of the ECHR. In the words of this provision, "(e)veryone has *the right to respect for his private and family life*, his home and his correspondence". The EU Charter of Fundamental Rights[15] mirrors Article 8 of the ECHR in its Article 7, which establishes that "(e)veryone has the right to respect for his or her private and family life, home and communications".[16] As the rights contained in the Charter's Article 7 correspond to those comprised by Article 8 of the ECHR, they need to be interpreted as having the same meaning and scope – as mandated by the Charter's horizontal provisions.[17]

The European Court of Human Rights has repeatedly maintained that the right to respect for private life recognised in Article 8 of the ECHR needs to be interpreted by recognising that 'private life' is a broad notion. Arguing that it 'does not consider it possible or necessary to attempt an exhaustive definition' of the notion, it has nevertheless emphasised that it would be 'too restrictive' to limit its scope of protection to an 'inner circle' in which individuals may live their lives without developing relationships with others,[18] and has stressed that there is no reason of principle to sustain that the notion of 'private life' shall be taken to exclude professional or business activities.[19] With these observations, it has significantly minimised the possible relevance of the private/public dichotomy for determining the scope of 'private life', and tended instead to conceive of the right to respect to private life as protecting the freedom to live a life of one own.

The notion of 'private life' has been notably extended through its contiguity with the other rights mentioned in Article 8(1) of the ECHR. The Strasbourg Court has for instance maintained that telephone, fax and e-mail communications are covered by the notions of 'private life' and 'correspondence',[20] and thus not solely through the latter. And under this broad notion of 'private life', the Strasbourg Court has included the protection of individuals

---

Perspective, Cambridge, MA: MIT Press; Solove, D.J. (2008) *Understanding Privacy*, Cambridge MA: Harvard University Press.

[14] These notions and the relations between them have been notably studied in PRISMS D5.1, D5.2 and D5.3.

[15] Charter of Fundamental Rights of the European Union, OJ C 83,30.3.2010.

[16] The second paragraph of Art. 8 ECHR is regarded as covered by Art. 52(1) of the Charter, which specifies that limitations to the exercise of EU fundamental rights are possible if, subject to the principle of proportionality, they are necessary and genuinely meet the objectives of general interest of the EU – which can certainly include security – and if they are provided for by law and respect the essence of those rights and freedoms.

[17] Concretely, Art. 52(3) EU Charter.

[18] *Niemietz v Germany,* Judgement of the Court of 16 December 1992, Series A no. 251-B, para 29.

[19] Ibid.

[20] See, for instance, *Liberty and Others v. The United Kingdom*, Judgment of 1 July 2008, Application no. 58243/00, Strasbourg, para 56.

against the processing of data related to them.[21] Taking the wording of Article 8 of the ECHR as a starting point, the Court has had recourse to ideas that originated in data protection law both to broaden the scope of Article 8(1) ECHR, and to refine its assessment on the possible lawfulness of interferences as per Article 8(2) ECHR. In EU law, however, this protection against data processing through Article 8 of the ECHR has been flanked since 2000 by the recognition of another right, the EU fundamental right to the protection of personal data.

8.2.2 Personal data protection

Until relatively recently, there was some reluctance in the literature to consider personal data protection as a notion fully separate from privacy, and thus to engage in any discussion of its conceptualisation as an autonomous legal concept. The recognition in 2000 by the EU Charter of a fundamental right to the protection of personal data (in Article 8) different from the right to the respect for private life (in Article 7) was a major stimulus to reconsider such position, even though the legacy of decades of envisioning personal data protection primarily through the frame of privacy is still palpable in most of the discussion around it.[22]

Nowadays, the right to privacy and the right to the protection of personal data are more widely acknowledged as separate notions.[23] This leads to the question of what is the specific nature of personal data protection – an issue on which there is, as a matter of fact, no consensus. Existing understandings of the European right to the protection of personal data typically oscillate between two poles: one approach envisages the right as representing, in substance, an overall prohibition against the processing of personal data (which could be labelled a *prohibitive* notion), whereas another view conceives of the right as constituting instead, in essence, a series of rules applying to the processing of personal data, regulating and limiting such processing but not forbidding it [or as a *permissive* (or regulatory) notion].

Constructing a picture of privacy and personal data protection as two distinct entities sometimes also highlights the similarities between them. This understanding often sustains the vision of personal data protection as a general prohibition of the processing of data about individuals.[24] Sometimes, however, scholars and jurists have put forward a conception of personal data protection as essentially divergent from privacy. An exemplar of such a characterisation is the categorisation of privacy and data protection in terms of *opacity v. transparency* tools. From this perspective, the basic feature of privacy would be that it aims to protect individuals by saturating their opacity in front of power, drawing normative limits,[25] whereas the key feature of data protection would be that its aim is to reinforce the transparency of power's exercise by organising and regulating the ways any processing of

[21] See among others: *Leander v. Sweden*, 26 March 1987, § 48, Series A no. 116; *Amann v. Switzerland* [GC], no. 27798/95, § 69, ECHR 2000-II; *Rotaru v. Romania*[GC], no. 28341/95, § 55, ECHR 2000-V. See also De Hert, Paul, and Serge Gutwirth, "Data Protection in the Case Law of Strasbourg and Luxembourg: Constitutionalisation in Action", in Serge Gutwirth, Yves Poullet et al. (eds.), *Reinventing Data Protection?*, Springer, Dordrecht, 2009, pp. 3-44.

[22]The Charter became legally binding only in 2009 but it was already influential before, since its proclamation (when references to the Charter started to appear in EU secondary law) and then even more since the signing of the Lisbon treaty in 2007

[23] See, for instance, Hustinx, Peter J., "Data Protection in the European Union", *P&I*, 2005, pp. 62-65. www.edps.europa.eu/.../EDPS/.../05-04-21_Data_Protection_EN.pdf

[24]Blume, Peter, "Lindqvist Revisited – Issues concerning EU data protection law", in Henning Koch (ed.), *Europe: the new legal realism: essays in honor of Hjalte Rasmussen*, DJØF, Copenhagen, 2010, p. 86.

[25]De Hert, Paul, and Serge Gutwirth, "Privacy, Data Protection and Law Enforcement: Opacity of the Individuals and Transparency of Power", in Erik Claes, Antony Duff and Serge Gutwirth (eds.), Privacy and the Criminal Law, Intersentia, Antwerp-Oxford, 2006, pp. 61-104; and Gutwirth, Serge, "Biometrics between opacity and transparency", Annali dell'Istituto Superiore di Sanità, Vol. 43, No. 1, 2007, pp. 61-65.

personal data must be carried out in order to remain lawful.[26] Privacy and data protection would thus by default serve divergent rationales, even if they can be punctually coincidental.[27] Data protection as such would not aim at protecting against data processing, but only from some unlawful data processing practices.[28] This view appears to fit what some have called a *permissive* notion, in the same way as other depictions of data protection as offering positive and dynamic protection (at variance with the negative and static protection of privacy).[29]

8.3 BACKGROUND MATERIAL ON PARTICIPATIVE APPROACHES AND EVIDENCE GATHERING

The PRISMS DSS is intended to support the incorporation of insights and perspectives drawn from participatory research methods into the security decision-making process, alongside the structured analysis of privacy issues. The aim of this section is provide an initial introduction to this form of information gathering activity for those users of the DSS who might be unfamiliar with it, and point to additional resources in this area.

Participatory research methods refer broadly to any information gathering activity which seeks to involve people (often users, stakeholders or affected parties) as active participants in the process. The aim for the decision maker is to gain access to perspectives and insight that they might not otherwise have, and supplement "insider" and "expert" knowledge with that held by other parties. For the participants, these activities offer an opportunity to participate in a security decision which may affect them, and to make decision makers aware of their hopes, concerns, and other forms of input.

One of the advantages of some participatory methods is that they can allow for interaction amongst the participants, rather than simply between participant and researcher. This is particularly useful for surfacing differences in opinion and conflicts. The participatory methods listed below run along a spectrum from the lower levels of intra-participant interaction to higher levels. There is also a parallel order in terms of administrative overheads (for example, the difficult of bringing together a large number of stakeholders. Participatory research shifts into the related terrain of participatory design[30] when external parties are brought into the design of security measures in more detail (rather than providing perspectives on alternatives devised or selected by the project team).

Each of these methods could be used to solicit information in support of key stages of the DSS. In particular for potential infringements of privacy (5.2) and Individual, group and categorical impacts, (5.6). Each of these approaches carries an ethical responsibility for the security decision maker as researcher, even in the structured context of the decision support system. Participants should be provided with full information about the purpose of the activity and how their contributions will be used, and participants should be allowed to withdraw their consent to participate. Considerations about confidential handling and anonymisation of data collected should be implemented.

---

[26] Ibid., p. 62.
[27] Ibid., p. 63.
[28] De Hert and Gutwirth, op. cit., 2009, n, 21, p. 3.
[29] Rodotà, Stefano, "Data Protection as a Fundamental Right", in Serge Gutwirth, Yves Poullet et al. (eds.), *Reinventing Data Protection?*, 2009, pp. 77-82.
[30] Spinuzzi, Clay., "The methodology of participatory design", *Technical Communication,* Vol 52, No. 2 May 2005, 163-174.

8.3.1 Interviews

Unlike the other methods, interviews (in the form of questionnaires and surveys as well as over the phone), can be conducted remotely. Interviews are also useful when expert information is required on a particular topic. The DSS works best with *semi-structured interviews* where a number of key questions (based upon the DSS templates) are prepared in advance, but the interviewer brings enough flexibility to be able to capture additional, unforeseen information from the interviewee. Interviews should therefore ideally be conducted by somebody with knowledge of the DSS and of the security threat and measures

8.3.2 Focus groups

Focus groups are a method of conducting interviews that involves small groups of four or more people, focused on a particular theme, with interest in the way that members of a group discuss that theme or issue.[31] Interaction is an important component of focus groups.[32] These sessions are usually facilitated by a moderator, often with a question guide. The method has a long history in market research contexts, although these are often more structured than the more open methods found in social science approaches. The main purpose of focus group research is to draw upon respondents' attitudes, feelings, beliefs, experiences and reactions in a way in which would not be feasible using other methods, for example observation, one-to-one interviewing, or questionnaire surveys.[33] A key element of this is the opportunity to find out *why* an issue or factor is salient to the participants (in the PRISMS DSS for example - why does an individual find a particular security measure to be discriminating against them?).

Focus groups allow for relatively complex information, addressed directly to the topic of concern, to be acquired quickly and in a wide range of contexts. [3435] However, focus groups can be dominated by strong participants, and less confident participants can be silenced, although this can be balanced by professional moderation, and the demographic mix of participants should be carefully considered to ensure that diverse perspectives are included. Focus groups make it difficult to identify individual positions (given that these are articulated in a specific context) but as the DSS does not primarily seek this type of information the impact of this is low.

8.3.3 Workshops

Workshops generally involve experts and practitioners and often involve pre-prepared material upon which the participants are invited to comment on in detail, based upon their various areas of expertise. The workshop format is valuable because it allows for interaction and interchange between the participants which can highlight different perspectives and the reasons behind them. Workshops can be useful in support of the DSS particularly in generating alternative security measures, assessing the efficacy of security measures, and in identifying privacy impacts. The particular question or questions to be put to the participants should guide the selection of appropriate participants.

8.3.4 Town-hall meetings / Citizen summits

Town-hall meetings or citizen summits are large-scale gatherings, with the largest number of simultaneous participants.

---

[31] Bryman, Alan, *Social Research Methods,* Oxford, Oxford University Press, 2001.
[32] Kitzinger, Jenny, "The methodology of focus groups: the importance of interaction between research participants", Sociology of Health and Illness, Vol 16, No. 1, 1994.
[33] Gibbs, Anita, *Focus Groups*, Social Research Update, 19, Winter 1997, http://sru.soc.surrey.ac.uk/SRU19.html
[34] [find reference] http://www.sagepub.com/upm-data/39360_978_1_84787_909_7.pdf
[35] http://www.qualres.org/HomeFocu-3647.html

The SURPRISE project made use of citizen summits to learn about how people interpret the use of surveillance technologies in nine European countries. In each country, the researchers gathered together around 200 participants in public meetings for face-to-face conversations. The researchers also made use of anonymous electronic voting technology to gather responses to several questions.[36]To gain deeper insight into participants' opinions, the SurPRISE summits were based on a mixed approach combining quantitative and qualitative elements. In detail, a set of pre-defined questions and statements clustered around different topics was complemented by discussion rounds relating to such thematic blocks[37]

Participants in town hall meetings are often provided with some stimulus information, either in advance of the meeting of at the start of the day. Citizen summits may be broken down into tables of smaller groups, moderated in a similar manner to concurrent focus groups, although the group can come back together for information sessions and plenary discussions.

8.4 DATA PROTECTION AND PRIVACY DESIGN PRINCIPLES

8.4.1 Privacy principles

Internationally, the *OECD Privacy Principles* provide the most commonly used privacy framework, they are reflected in existing and emerging privacy and data protection laws, and serve as the basis for the creation of leading practice privacy programs and additional principles. The *OECD Privacy Principles* tie closely to European Union (EU) member nations' data protection legislation (and cultural expectations), which implement the European Commission (EC) Data Protection Directive (Directive 95/46/EC), and other "EU-style" national privacy legislation. The OECD Privacy Principles, the Fair Information Principles and the principles used in the Convention of the Council of Europe 108 all resemble each other and imply the following principles:

Collection limitation principle - There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

Data Quality principle - Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

Purpose specification principle - The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

Use limitation principle - Personal data should not be disclosed, made available or otherwise used for purposes other than those specified except: a) with the consent of the data subject; or b) by the authority of law.

Security safeguards principle - Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

[36]Skov, Emma Christiani& Anne Kristine Smith Lygum, *D5.4 - Evaluation of Citizen* Summits, June 2014, http://surprise-project.eu/wp-content/uploads/2014/10/SurPRISE-D5.4-Evaluation-of-the-Citizen-Summits.pdf
[37]Straβ, Stefan, D6.12 - Workshop Report, SURPRISE project, December 2014, http://surprise-project.eu/wp-content/uploads/2015/02/SurPRISE-D6.12-Workshop-report.pdf

Openness principle - There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

Individual participation principle - An individual should have the right: a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; b) to have communicated to him, data relating to him i) within a reasonable time; ii) at a charge, if any, that is not excessive; iii) in a reasonable manner; and iv) in a form that is readily intelligible to him; c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

Accountability principle - A data controller should be accountable for complying with measures which give effect to the principles stated above.

8.4.2 Privacy by design

Privacy by design is loosely defined concept at this moment. A number of authors offer approaches towards operationalizing privacy by design in systems architecture, in services and in products. Again, a distinction needs to be made between privacy by design and data protection by design. DP by design is introduced in the GDPR, referring to accepting the data protection principles in the early phases of project design. Essentially it refers to appropriate technical and organisational measures to assure the protection of personal data already in the design phase (and not as an add-on). Tools for data protection by design are available, such as encryption tools and pseudonymization techniques, or TTPs for organisational measures (in combination with technical measures such as encryption and pseudonymization). http://www.privacybydesign.ca/, http://ico.org.uk/for_organisations/data_protection/topic_guides/privacy_by_design

The seven Foundational Principles of privacy by design as developed by the Canadian Privacy Commissioner are:

1. Proactive not Reactive; Preventative not Remedial
2. Privacy as the Default setting
3. Privacy embedded into design
4. Full functionality – Positive-sum not Zero-sum
5. End to end security – lifecycle protection
6. Visibility and transparency – keep it open
7. Respect for privacy – keep it user-centric.

(http://www.privacybydesign.ca/index.php/about-pbd/7-foundational-principles/)

Co-ordinator:
Dr. Michael Friedewald
Fraunhofer Institute for Systems and Innovation Research ISI
Breslauer Straße 48 | 76139 Karlsruhe | Germany
Phone: +49 721 6809-146 | Fax +49 721 6809-315
michael.friedewald@isi.fraunhofer.de