Project acronym:	CRISP
Project title:	Evaluation and Certification Schemes for Security Products
Grant number:	607941
Programme:	Seventh Framework Programme for Security
Objective:	Topic SEC-2013.5.4-1 Evaluation and certification schemes for security products
Contract type:	Capability project
Start date of project:	01 April 2014
Duration:	36 months
Website:	www.crispproject.eu

Deliverable D4.2:
Ethical Expert Report on Freedom Infringement Evaluation

Authors:	Daniel Neyland (Goldsmiths University of London), Irene Kamara, Paul de Hert (Vrije Universiteit Brussel) *with contributions from the CRISP consortium.*

Dissemination level:	Public
Deliverable type:	Final
Version:	1.0.
Submission date:	30 April 2015

Table of Contents

1 INTRODUCTION

This report is part of Work Package 4, which focuses on analysis of the core dimensions, security, trust, efficiency and freedom infringement (STEFi), with regard to security products, systems and services. The Work Package aims to analyse existing schemes and standards to identify evaluation criteria based on the four core dimensions and come up with requirements for further development, enhancement, adaptation and integration of evaluation and certification schemes of products used for security purposes. The Work Package also aims to identify and analyse core issues associated with certification.

The Work Package 4 consists of three deliverables: 1) The Legal Analysis of Existing Schemes[1] 2) The Ethical Expert Report on Freedom Infringement Evaluation 3) The STEFi based SWOT Analysis of Existing Schemes[2].

More specifically, the ethical expert monitored and advised the consortium on the task on freedom infringement evaluation. The task examines the impact of technologies and measures on the freedoms of people. These freedoms include: bodily integrity, equal treatment and non-discrimination, freedom of movement, freedom from unlawful detention, presumption of innocence, fair trial and due process, privacy and data protection.

The task aims to operationalise the freedom infringement dimension by providing evaluation criteria that are appropriate to evaluate security products or services. This task elaborates on the work done in the SIAM-project, as well as incorporating the results of other projects concerning the impact of technology on privacy like PRISE, SAPIENT, PIAF and Prescient. The analysis of the freedom infringement task is in both the Legal analysis and STEFi based SWOT Analysis deliverable, as it will be further explained in the relevant chapter of this report.

This deliverable contains the report of the ethical expert appointed to monitor and advise the consortium on Task 4.4 (freedom infringement evaluation) and includes a report of the measures or actions taken by the consortium in response to the advice provided by the ethical expert in D4.2. The deliverable also encompasses other measures taken to comply with the recommendations from the ethical expert.

In more detail, the report is developed as follows:

Chapter 1 introduces the reader to the aim of this report and the relation to Work Package 4 and CRISP.

Chapter 2 contains the report of the ethical expert on the freedom infringement evaluation.

[1] The Legal Analysis of Existing Schemes Deliverable is to be published by 30th April 2015.
[2] The STEFi based SWOT Analysis of Existing Schemes Deliverable is in progress.

Chapter 3 enlists the measures and actions taken by the consortium in order to implement the advice provided by the ethical expert in relation to freedom infringement evaluation and other advice in relation to other aspects of the analysis.

Chapter 4 provides a summary of the reports and concluding remarks.

2 THE ETHICAL EXPERT REPORT

2.1 INTRODUCTION

This section of the deliverable contains a summary of the advice thus far provided by the ethical expert for CRISP, Professor Daniel Neyland. The advice contained in this section is preliminary and is provided on the basis of making a constructive contribution to the reports produced by the consortium. As ethical expert, I look forward to receiving further future reports on which I can make further contributions. This section of the Deliverable is designed to fulfil the remit of Task 4.4 of the CRISP consortium as specified in the Description of Work. This section of the report begins with a summary of my advice on the general tasks of CRISP. It then proceeds to present my advice on freedom infringement and the STEFi criteria. Following this is a summary of the advice offered on other aspects of CRISP work. This section concludes with a list of requirements drawn up based on the advice offered.

2.1 GENERAL ADVICE ON CRISP TASKS

The main task as I understand it in the CRISP consortium is to produce a set of criteria for assessing security, trust, efficiency and freedom infringement (STEFi), with regard to security products, systems and services. My initial and general suggestion was that these criteria should begin from the current legal position and the development of the new Data Protection Regulation. However, I also suggested that such criteria can go beyond regulations and a key task of an 'ethics' advisor, in comparison to for example a legal advisor, is to look beyond law alone to also investigate what further issues might require consideration. I hence suggested that the consortium ought to look at privacy reports and assessments, other FP6 and 7 projects, and other relevant projects. These could be assessed for what they might offer in terms of criteria that are perhaps legally embedded but also go beyond the law.

However, I suggested that a key task for CRISP, is how to make a set of evaluation criteria relevant to a broad range of security products. Attempting to make a single set of criteria carries with it a number of risks:

One risk is that the criteria is so broad that a great deal of work has to be done to make the criteria relevant to many security technologies. For example, a fence might be a security technology that limits freedoms and a security justification might be given for using algorithmic data mining technologies to sift through my on-line communications in order to at some point in the future restrict my freedoms to be on-line, to share data, to interact with certain other parties and so on. The form of freedom infringement and CRISP criteria of assessment has to be made to make sense in relation to the details of the technology under consideration. A broad and general criteria in this sense does not make life easier for those

designing, developing, selling or using security technologies; ambiguities might remain about what the criteria mean to specific technologies if they are drawn too broadly.

An alternative risk, is that the criteria is too narrow - in this case, a security technology could 'fail' on the terms of the evaluation criteria, but only because it is not the type of security technology which fits the criteria. If things like Privacy Enhancing Technologies are subject to the same evaluation criteria as more basic security technologies, the more basic technologies (like fences or lighting) might not score well on the criteria, but at the same time this might not be a problem for the technology or the public - it might be a problem with having a single, narrowly drawn criteria.

My suggestion to manage these risks is to produce something more complex than a single list of criteria.

My suggestions for going beyond a single list of criteria are based on the assumption that freedom infringements are likely to vary between different security technologies. For example, CCTV cameras will potentially infringe freedoms in different ways and to different extents than, for example, locked doors or security lighting. Even within CCTV, there are digital, networked cameras, remotely accessed, more traditional systems with fewer digital components or at the other end of the technological spectrum, camera systems tied to 'smart' or algorithmic analytic systems. The types of freedom infringements, and for whom freedom would be infringed, would be very different for different technologies.

Given the aforementioned risks involved in drawing up a too narrow or too broad set of criteria and the difficulty of having a single list of criteria that would classify all relevant freedom infringements for all security technologies, it would seem advisable to organise the criteria into a matrix. In this matrix the types of technology would need to be made clear in detail (i.e. not just CCTV, but the type and sophistication of CCTV), then the freedom infringements that were specific to that technology would need to be made clear (i.e. not the whole list of every infringement, just the ones relevant to that technology) and then a third dimension would have to be for whom there was a risk of freedom infringement (i.e. staff working in a secure space, operators of security equipment, different public groups, etc). A fourth dimension would then have to be the measure taken to protect against that freedom infringement or at least how this would be assessed. A fifth criteria would be how the measures and compliance with the measures would be made accountable and to whom. A sixth criteria would be how any form of redress would be offered or managed to those who still felt their freedom had been infringed despite the protections in place. These might each be different for different security technologies.

My final general suggestion to the CRISP consortium was that the results from the criteria ought to be made available to those interested in the data. In this way, the extent of compliance with specific criteria details, whom might be at risk of having their freedom infringed, could be accessed. I suggested there was both a short-term and a long-term approach to making such information available. A short-term approach would involve ensuring that project results are made available in all the usual ways (publications,

presentations, websites). The long-term approach would involve the CRISP system under development taking into account who the beneficiaries of the system should be and how they could be incorporated into a form of accountability that allows them to know that the system exists, is working on their behalf and incorporates a form of redress.

2.2 FREEDOM INFRINGEMENT AND THE STEFI CRITERIA

Moving on from my general comments on the CRISP project, I was tasked with looking at the issue of freedom infringement in particular. This is important as an aspect of the CRISP project and a key ethical criteria for assessing security technologies and their design, development and deployment. Freedom infringements pose a number of risks to those subject to, for example, security technologies with data collection components or security technologies designed to prohibit, for example, free bodily movement or entry or exit from a particular space. As a concept, freedom infringement also poses risks for those setting criteria to assess security products. What counts as a freedom infringement, for whom, in what place, at what time and with what consequence each appear to be valid questions to pose. In line with my general comments above, the CRISP project will need to develop a sophisticated means to deal with what might otherwise be an elusive concept or a criteria which shifts inordinately between different situations, different technologies or different locations. The public sensitivity to freedom infringement is also likely to shift between different places and actions.

Reading the draft deliverable section on freedom infringement, I was reassured that in general the report was comprehensive and detailed. The CRISP consortium had clearly worked hard to draw together a range of relevant materials that raised relevant issues for freedom infringement in relation to security technologies. The deliverable section provided a clear sense that freedom infringement is not a singular issue, but requires subtle and sophisticated handling. The details in the deliverable on bodily integrity, equal treatment and non-discrimination, freedom of movement and freedom from unlawful detention, presumption of innocence, fair trial and due process, privacy and data protection were all welcomed.

Having introduced the complexities of freedom infringement as a concept, the CRISP consortium will now have to incorporate those complexities into the project's assessment criteria for security technologies. My suggestions for the consortium can hopefully prove of use towards this goal. Bodily integrity, for example, will only be an issue for certain types of security technology, whereas equal treatment and non-discrimination might be an issue of more pervasive relevance. At the same time, both issues will vary significantly between, for example, more basic security technologies (lighting and fencing) and more sophisticated technologies (CCTV, on-line tracking). Freedom of movement is in itself a complex issue and will need to be treated with care in relation to security products. It is not the case that individuals can freely move anywhere and the central purpose of many security products is to legitimately prevent either the movement of people into a space or the movement of things into or out of a space. In translating this into a criteria to assess security technologies, a range

of initial questions will be required to ensure the assessments being made of particular security products are relevant to those security products and the users or others who might come into contact with them. The issue of fair trial and due process seems of great import again as a basis for considering freedom infringements, but will only be relevant to certain security technologies in certain situations. Privacy and data protection will also be mostly relevant for more sophisticated security technologies. However, given the complexity of privacy and on-going developments in data protection, the consortium will have to be flexible in how they deal with these issues. Finally it seems worth pointing out that each of these concerns can be transformed again by combinations of security technology. Freedom infringements posed by CCTV might look quite different when or if digital CCTV footage were combined with, for example, on-line data mining and scraping technologies.

Central to the CRISP consortium in managing these issues will be the STEFi criteria it seems. On reviewing these criteria I was on the whole satisfied that they were moving the project in the correct direction. However, given that they seem to have a central role in the development of the project and its likelihood of achieving the ambitious objectives it has set, I felt there were a number of areas of the criteria that required some attention. I will introduce these areas here and also summarise my suggested recommendations for change in a following table.

These comments each related to the initial version of the criteria that were sent to me at the end of 2014 and early in 2015 and were subsequently worked on by the consortium. Initially I was struck by the term 'attributes' in the criteria table. This term seemed unclear to me and bore little relation to the content it headed. I suggested that the consortium address the meaning of the term 'attributes'.

Staying with the table headings, it was also unclear to me why there was a column titled STEFi dimensions with a series of numbers in the column. Presumably this plays a practical role for the consortium, but as a standalone document it is difficult to comprehend.

The role of qualifying questions (as I mentioned previously) also seemed central to the way in which the criteria might work. For example, if it follows that certain criteria are only relevant to certain technologies, or combinations of technology, or certain deployments of technology, then these need to be reflected in initial qualifying questions. Otherwise a technology might pass or fail the criteria or be assessed by the criteria in an irrelevant manner.

Under the criteria for freedom infringements, I also thought a number of further criteria might be required, depending on the security technology, its sophistication, and use. These included: Data storage (for how long might data be stored, is it stored securely, by whom, assessed how, deleted when?); Accountability (for whom, by whom, using what means with what consequences?); Transparency (how for example the presence and operation of a technology might be made apparent); Commodification of data (for example, with increasing focus on the use of technologies to make something new from digital data in order to take it to the market, raising questions about the origins, ownership and privacy consequences of

data, how might this be translated into an assessment criteria?); Data transfer (for example between data owners, across the EU and beyond the EU); Third parties (for example, with the rise of social media comes a plethora of new security products but also security concerns – about third party data ownership and about third party data access); Automated decision making (for example with algorithms either automating or semi-automating decision making processes in certain security environments, what might this mean for freedom infringements?).

Alongside what I perceived to be missing dimensions (listed above) were a number of areas that seemed to require some clarification. First, consent appears in the criteria, but this is a difficult criteria to achieve. Often, 'consent' means no more than notice (e.g. that a data subject is notified that a technology is in operation, not that they are expected to or have the opportunity to explicitly consent or withhold consent from the operation of, for example, CCTV). Second, function creep was mentioned in the criteria, but every technology can be used for another purpose. The question here should be, how have safeguards been put in place to protect against Function Creep? And another question: Have changes in technology use been made transparent to data subjects? Third, much was made in the draft deliverable on freedom infringements about bodily integrity and drones, but neither seemed to manifest in a particular question in the criteria.

In the following table, my suggestions to the CRISP consortium thus far are summarised:

Summary Recommendations on Freedom Infringements and the STEFi Criteria
The criteria should begin from current legal position
Include General Data Protection Regulation
Look at privacy reports and assessments; other FP6 and FP7 projects
Introduce something more complex than a single list of criteria e.g. a matrix, in order to address the issue of too narrow or not relevant. Address the risk of security technologies failing because there it is not the type of technology which fits the criteria.
Address the risk of how to make a set of evaluation criteria relevant to a broad range of security products
Types of technology should be made clear, and the sophistication of technology
Address the issue for whom there might be a risk of freedom infringement or at least how this should be assessed
Accountability: how the measures would be made accountable and for whom
Include a form of redress mechanism
Clarify what "attributes" in the table of evaluation criteria means
Clarify what are the STEFi numbers on the table
Include qualifying questions to assess if criteria are relevant to a particular technology. How/where would these qualifying questions work?
Include questions related to:

• data storage • accountability • transparency • commodification of data • data transfer and third parties • automated decision making
The concept of consent should be clarified (does this mean notification or a request to give consent?)
Under the term function creep the question should be rephrased: how have safeguards been put in place to protect against function creep? Add: have changes in technology use been made transparent to data subjects?
Include a question on bodily integrity
include a question specifically related to drones

2.3 Other Issues in WP4

Although the preceding sections highlight the main comments I had on the tasks of the CRISP consortium in general and the freedom infringement and its relation to the STEFi criteria, I also raised a small number of further points in relation to security, trust and efficiency. Partly, these took the form of questions for the consortium and partly they took the form of further suggestions that the consortium might consider.

Security: According to the version of the criteria that I assessed, under the heading security, the consortium were hoping to gather some data in order to assess what was termed 'deviance.' It was unclear to me what this might involve. Although deviance has a long standing as a term used in sociology, often to connote forms of activity that are either on the fringes of criminality or not criminal but perhaps questioned in terms of their social acceptability by some, how would this relate to the certification of security technologies? The criteria also seem to posit a link between limitations and risk - why are these terms combined together?

Trust: This is another term with a long standing in sociology and other social sciences. I won't attempt to summarise 50 years of research here, but the important question for the consortium is what particular understanding of trust is central to the criteria. It seems that trust is designed to capture some quite important aspects of the relationship between a security product and those deploying it and those subject to the technology. Under the psychological section of the criteria on trust, it appears to suggest that any organisations or technologies that have a negative impact on anyone with a phobia would be scored badly. But how would this be scored? And what would it say of a technology if one person had a phobia of it? Trust here seems to require some more extensive detailing.

Efficiency: This term is used in the criteria for what seem to be two different purposes. There is a mix of the economic sense of efficiency and a more practical sense of efficacy or effectiveness both used under the same heading in the criteria. Although this does not seem as

central as trust is to the assessment of the ethics of the criteria, the combination of terms might still have some consequence. The consortium should be clear on the use of this term.

The following table summarises my recommendations beyond the freedom infringement aspects.

Summary of Other Recommendations
The consortium should define the audience for evaluations (public, security firms, regulators)
The consortium should make results available in the short term through publications, presentations and websites.
The consortium should make results available in the long-term: by taking into account beneficiaries and how they can be incorporated in a form of accountability that allows them to know that the system exists, is working on their behalf and incorporates a form of redress
Security evaluation: under accuracy, what does sensibility mean?
Security evaluation: What type of data are you hoping to gather in relation to deviance?
Security evaluation: Why risks and limitations together?
Trust evaluation: what does it mean to say under observation that the attribute is expression?
Trust evaluation: under psychological section, are you expecting organisations to demonstrate that they will not cause any negative impact on anyone with a phobia? How could they do that?
Efficiency evaluation: criteria are a mix of economic sense of efficiency and a more practical sense of efficacy or effectiveness - is it sensible to group together?

3 REPORT ON MEASURES TAKEN IN RESPONSE TO THE ADVICE OF THE EXTHICAL EXPERT

This report presents the actions undertaken by the consortium in order to comply with the ethical expert advice in relation to the freedom infringement evaluation and other tasks of the WP4 on the core dimensions – security, trust, efficiency and freedom infringement- of certification and evaluation of security measures. The first part includes actions in relation to the advice of the ethical expert with regard to the freedom infringement evaluation. The second part of this chapter includes the measures and actions taken by the consortium to implement other advice and guidance provided by the ethical expert of the CRISP project.

3.1 ACTIONS IN RELATION TO FREEDOM INFRINGEMENT EVALUATION TASK

With regard to the Freedom Infringement task, the ethical expert monitored the work closely from the beginning and provided useful advice and guidance. In this chapter we list the advice and the relevant action or measure of the consortium.

1. *Requirements should start from legal position*

In the Legal Analysis of existing schemes deliverable (D.4.1.), we address the issue of core requirements of the security products, systems and services and accordingly their evaluation and certification schemes, primarily from a legal perspective. For each examined aspect, and in particular the freedom infringement aspect, there is a comprehensive analysis of the relevant legislation.

As the CRISP Description of Work required, the partners examined the right to personal data protection and privacy, the freedom of movement and freedom from unlawful detention, the presumption of innocence, the right to equal treatment and non-discrimination, the fair trial and due process right and the right to bodily integrity. By looking at the European Convention of Human Rights[3], the Charter of Fundamental Rights of the European Union[4] but also the secondary legal instruments regulating the above rights and providing safeguards on their protection, such as Directives, Regulations any in specific cases, such as drones, the national legislation, the legal analysis deliverable provides insight on what is the regulatory framework, what are the core obligations and requirements of the legislation for the security measures and how the security products, systems and services might challenge and violate each one of the above rights and freedoms. The analysis also examined the impact of technologies which are employed in security measures in the potential infringement in particular of the right to private life and freedom infringement.

[3] Council of Europe, Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) (ECHR)
[4] European Union, Charter of Fundamental Rights of the European Union, December 2000, Official Journal of the European Communities, OJ C 364/01,(18.12.2001)

2. *General Data Protection Regulation should be included in the analysis*

The freedom infringement chapter of the Legal Analysis of Existing Schemes Deliverable includes a section analysing the provisions of the draft General Data Protection Regulation[5] and the suggested amendments by the European Parliament (LIBE Committee)[6]. Moreover, the SWOT Analysis Deliverable of Existing Schemes also includes criteria and requirements derived from the proposed text of the General Data Protection Regulation, such as the Data Protection Impact Assessment. Although the text of the Regulation is not final yet, the CRISP project needs to follow the developments in the legislation, in specific on the protection of freedoms and human rights, which have an important impact on the scrutinised citizens.

3. *Look at privacy reports and assessments and other FP6 and FP7 projects*

Both deliverables take into account the important research and results of other EU projects. The STEFi methodology employed in the Work Package 4 was first developed in the SIAM project[7]. CRISP takes the methodology one step further by adapting it to the needs of evaluation and certification schemes of security products, systems and services. The research team also did a comprehensive analysis of the projects PRISE[8], SAPIENT[9], PIAF[10] and Prescient[11] and incorporated the results into the analysis of the four dimensions of the STEFi methodology. The projects were also very useful in providing sources for requirements and criteria for the evaluation of security products, systems and services, as well as for the typology of technologies used in security products, systems and services and their impact in relation to the examined freedoms and human rights. The SWOT analysis deliverable also presents a showcase of the DESSI project[12].

4. *Types of technology should be made clear, types of sophistication of technology. Address the risk of security technologies failing because it is not the type of technology which fits the criteria.*

The different capabilities of technologies have an influence on the invasiveness and violation of the freedoms and rights; the use of a CCTV system with a rotating camera has more

[5] Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD))
[6] Report of the European Parliament on the Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), (COM(2012)0011 – C7-0025/2012– 2012/0011(COD)), 22 November 2013, Committee on Civil Liberties, Justice and Home Affairs
[7] For the deliverables and reports of the SIAM project, see: http://www.tu-berlin.de/ztg/menue/forschungsbereiche_und_projekte/projekte_-_abgeschlossen/security_impact_assessment_measures_siam
[8] See website of the PRISE project: http://www.prise.oeaw.ac.at/
[9] See website of the SAPIENT project: http://www.sapientproject.eu/
[10] See website of the PIAF project: http://www.piafproject.eu/
[11] See website of the Prescient project: http://www.prescient-project.eu/prescient/index.php
[12] See website of the DESSI project: http://securitydecisions.org/about-dessi/

capabilities to violate the right to private life than a stable pan, tilt and zoom camera. The partners have examined the different types of technologies in Deliverable 1.2., the Taxonomy of security products, systems and services[13] and Deliverable 1.1. of the CRISP project, Glossary of security products and systems[14]. In the Legal Analysis Deliverable, the impact of the technologies of the security measures examined as case studies is analysed with regard to freedoms and rights. Moreover, in order to address the above issue, each criterion in the SWOT Analysis deliverable is characterised as technology neutral or technology specific, in order to provide additional tools of assessment of the security products, systems and services. At this point, it should be noted also the fact, that legislation protecting freedoms and human rights is technology neutral, in the sense that its applicability does not depend on the type or sophistication of technology. As a result, from a legal perspective, the technology factor is important to assess the impact of the security measure on the relevant freedom or right, but not to determine how the legislation protects the rights under threat and what are the obligations of the accountable parties. In this case, it is quite often that the *use* of the different possibilities that the technology offers that affects the applicability of the legislation, rather than the technology itself. It is true however that technologies might be more privacy intrusive than others. For example X-ray backscatter bodyscanners that reveal "people in such a way that is normally reserves for the private sphere" pose greater risk to the right to privacy of the scrutinised than the scanners employing privacy-enhancing software[15]. Although the question on how to address the issue of diverse technologies of security PSS in evaluating such security PSS is related to the CRISP methodology and thus beyond the scope of this Work Package, the consortium will further consult the ethical expert on the issue.

5. *Introduce something more complex than a single list of criteria in order to address the issue of too narrow or not relevant.*

The STEFi methodology of the SIAM project evolves in the context of CRISP. The methodology will be described in the SWOT Analysis deliverable. Criteria and attributes emerged at all times which can be structured into four dimensions that form the core of SIAM's security technology assessment procedure: Security, Trust, Efficiency and Freedom Infringements (STEFi).[16] Apart from the list of criteria for every aspect, there are attributes for each criterion. The role of attributes is to break down the criteria and explain the specific aspect of the criterion which is to be examined. To facilitate this, each attribute had relevant clarifying questions. Two more features address the advice by the ethical expert: a. the applicability/relevance question, which examines whether a criterion is relevant/ applicable in the case of the security measure under examination and b. the STEFi weights column, which

[13] Sveinsdottir Thordis, Finn Rachel, Rodrigues Rowena, Wadhwa Kush, Fritz Florian, Von Laufenberg Roger, Kreissl Reinhard, Tanas Alessia, Van Brakel Rosamunde, De Hert Paul, "Taxonomy of Security Products, Systems and Services", Deliverable 1.2 of the CRISP project, 2014

[14] Fritz Florian, Von Laufenberg Roger, Kreissl Reinhard, Tanas Alessia, Van Brakel Rosamunde, De Hert Paul, Wurster Simone, "Glossary of security products and systems", Deliverable 1.1 of the CRISP Project, 2014

[15] Van Brakel Rosamunde, Hildebrandt Mireille (2012) Literature overview of freedom infringements. from SIAM Deliverable 4.2., p. 17

[16] Hempel et al. (2013), p. 748.

by assigning for every criterion different weights to each aspect from a scale 0 to 3, indicate the interrelation of the criteria of one aspect to the other STEFi aspects.

6. *Address the issue for whom there might be a risk of freedom infringement or at least how this should be assessed*

The analysis focuses on the scrutinised citizen and the end user of the security product or system. The scrutinised, the person who is targeted by the security measure or undergoes the security control, is the primarily affected by the risks to freedoms and human rights that the security measure poses. Depending on the type of security measure, the scrutinised differs; in the case of a metal detector walk-through machine, the scrutinised is obviously the person passing through the machine. Identifying who is the scrutinised is not always so obvious; in the case of CCTV systems for crime prevention in public spaces, scrutinised is every person whose picture is captured by the CCTV cameras. The end users/operators of the security measure are also potentially a group that can suffer violation of their rights. This is especially for instance for the bodily integrity, when the security measure has potential impact to the health of the operator (also the scrutinised).

7. *Address the issues of data transfers and third parties, automated decision making in relation to protection of personal data, consent, accountability, transparency, data storage, redress mechanism.*

All of the above issues were inserted either as criteria, eg. redress mechanism, or as attributes to existing criteria eg. data protection in the Legal Analysis or SWOT Analysis deliverable, where appropriate. Additionally, the analysis supports and explains the rationale of the criteria and the requirements. The ethical expert also suggested questions in relation to function creep, which the consortium included in the SWOT Analysis deliverable.

3.2 ACTIONS IN RELATION TO OTHER ADVICE OF THE ETHICAL EXPERT

In the context of Work Package 4, the ethical expert of CRISP provided advice and guidance also for the security, trust and efficiency aspects, which partners implemented to the maximum possible extent, taking into also account the scope and objectives of the Work Package.

3.2.1 Security, trust and efficiency evaluation of Work Package 4

In relation to security aspect, the partners clarified concepts and criteria in the SWOT analysis deliverable, such as sensibility in relation to accuracy and others. Moreover, the criteria of risk and limitations with regard to the security products, systems, services were divided into different criteria.

In relation to trust, partners took into account the advice of the ethical expert by re-formulating or deleting attributes and criteria, such as attribute "claustrophobia" which was under the criterion "observability". The rationale for the deletion was that although the requirement is important for promoting trust and confidence of the scrutinised to the security products, it was however difficult to be measured as a requirement in a certification or evaluation scheme.

In relation to efficiency, the partners adopted the advice of the ethical expert to separate the requirements and criteria of the efficiency aspect and created accordingly two sub-categories for the efficiency aspect: a. General efficiency criteria, with a focus to economic sense and b. efficacy criteria, with a focus to more practical issues.

3.2.2 Dissemination activities for CRISP results

For short term dissemination, the CRISP project operates a website, where the deliverables of CRISP, relevant publications and other useful information related to the project are published [17]. The CRISP partners also attend events, either as speakers or participants, where they have the opportunity to inform interested parties on the work and objectives of CRISP. For long term dissemination, the ethical expert advised to take into account beneficiaries and how they can be incorporated in a form of accountability that allows them to know that the system exists, is working on their behalf and incorporates a form of redress. CRISP project held a stakeholder Workshop in December 2014 in Amsterdam in order to engage its stakeholders into the activities of the project and discuss with them the needs and priorities of the different stakeholder groups[18]. Other similar events are planned for the forthcoming months, engaging

[17] See CRISP project website: http://crispproject.eu/

[18] Read more on the Stakeholder Workshop and the stakeholder and end user survey: Sveinsdottir Thordis, Finn Rachel, Wadhwa Kush, Rodrigues Rowena, van Zetten Jolien, Wurster Simone, Murphy Patrick, Hirschmann

National Data Protection Authorities and Information Commissioners, a workshop on developing the certification methodology and others. The Work Package 8, focuses on dissemination and aims to identify stakeholders, their drivers and the best media to reach them and engage with them to promote the goals of EU-wide certification of security products.

Nathalie, Rallo Artemi, García Rosario, Pauner Cristina, Viguri Jorge, Kalan Eva, Kolar Igor, "Stakeholder Analysis Report", Deliverable 3.1. of the CRISP Project, 2015

4 SUMMARY AND CONCLUDING REMARKS

This Deliverable presented the ethical expert advice and the actions taken by the consortium to implement the advice. The ethical expert monitored closely the work of the consortium for the Freedom Infringement Task of the Work Package 4 and provided guidance and advice on the content and methodology.

Starting from advice on how to approach the task and which type of sources to include in the analysis, the ethical expert suggested to take into account regulations and existing legal texts, but also benefit from the research and results of other FP6 and FP7 projects and relevant sources. The analysis of the freedom infringement chapter in the Legal Analysis deliverable was approved by the ethical expert. The ethical expert also advised the consortium in relation to the core requirements (criteria) for the security products, systems and services in order to avoid developing too narrow or too broad criteria that are difficult to be implemented. To that end, the consortium took a series of actions, among which was the relevance/applicability question, which addresses the issue of relevance of the criterion in each case of security product, system or service, before proceeding to the actual examination of the requirement.

Suggestions were made also regarding the security, trust and efficiency dimensions of the STEFi methodology as applied to CRISP project; the consortium adopted the advice of the ethical expert and reformulated the requirements (criteria) accordingly.

To conclude with, the consortium welcomed the advice and guidance provided by the ethical expert and will continue to work in order to implement such advice from the ethical expert for the future Work Packages of the CRISP Project.

5 REFERENCES

Council of Europe, Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) (ECHR)

European Union, Charter of Fundamental Rights of the European Union, December 2000, Official Journal of the European Communities, OJ C 364/01,(18.12.2001)

Fritz Florian, Von Laufenberg Roger, Kreissl Reinhard, Tanas Alessia, Van Brakel Rosamunde, De Hert Paul, Wurster Simone, *Glossary of security products and systems*, Deliverable 1.1 of the CRISP Project, 2014

Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD))

Report of the European Parliament on the Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), (COM(2012)0011 – C7-0025/2012– 2012/0011(COD)), 22 November 2013, Committee on Civil Liberties, Justice and Home Affairs

Sveinsdottir Thordis, Finn Rachel, Rodrigues Rowena, Wadhwa Kush, Fritz Florian, Von Laufenberg Roger, Kreissl Reinhard, Tanas Alessia, Van Brakel Rosamunde, De Hert Paul, *Taxonomy of Security Products, Systems and Services*, Deliverable 1.2 of the CRISP project, 2014

Sveinsdottir Thordis, Finn Rachel, Wadhwa Kush, Rodrigues Rowena, van Zetten Jolien, Wurster Simone, Murphy Patrick, Hirschmann Nathalie, Rallo Artemi, García Rosario, Pauner Cristina, Viguri Jorge, Kalan Eva, Kolar Igor, *Stakeholder Analysis Report*, Deliverable 3.1. of the CRISP Project, 2015

Van Brakel Rosamunde, Hildebrandt Mireille, Literature overview of freedom infringements. from SIAM Deliverable 4.2., 2012