Document title:	**Ethical Best Practices guidelines.**
Due delivery date:	**24/01/2013**
Nature:	**Deliverable 7.3**
Project Title:	**Collaborative Information, Acquisition, Processing, Exploitation and Reporting for the prevention of organised crime**
Project acronym:	**CAPER**
Instrument:	**Large Scale Collaborative Project**
Thematic Priority:	**FP7-SECURITY-2010-1.2-1**
Grant Agreement:	**261712**

Organisation name of lead contractor for this deliverable:

Dissemination level		
PU	Public	
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	X

Proprietary rights statement
This document contains information, which is proprietary to the CAPER consortium. Neither this document, nor the information contained herein, shall be used, duplicated or communicated by any means to any third party, in whole or in parts, except prior written consent of the CAPER consortium.

Ethical Committee:

Dr. Danièle Bourcier (CNRS-Paris, Spain)

Josep Monserrat (UB, Barcelona, Spain)

Ugo Pagallo (UT, Torino, Italy)

Giovani Sartor (EUI, Florence, Italy)

John Zeleznikow (VU, Melbourne, Australia)

History			
Version	First name & Name	Modifications	Date
7.1.3 v1	Pompeu Casanovas	General framework and questioning on WP7 Deliverable 7.1.1	15/06/2012
7.1.3 v2	Ugo Pagallo	First Report on CAPER	29/06/2012
7.1.3 v3	John Zeleznikow	First Report on CAPER	30/10/2012
7.1.3 v4	Danièle Bourcier	First Report on CAPER	31/10/2012
7.1.3 v5	Giovanni Sartor	First Report on CAPER	25/11/2012
7.1.3 v6	Pompeu Casanovas	Ethics, Governance, and CAPER Regulatory Model (CRM)	15/12/2012
7.1.3 v7	Antoni Roig	Legal framework	15/12/2012
7.1.3 v8	Antoni Roig	Draft of Recommendations	15/12/2012
7.1.3 v7	Marta Poblet	Discussion	06/01/2013
7.1.3 v8	Pompeu Casanovas	Conclusions and further work	15/01/2013
7.1.3 v9	Pompeu Casanovas	Final version	21/01/2013

Validation			
	First name & Name	Organisation short name	Visa
Responsible	Antoni Roig	IDT-UAB	X
WP leader	Pompeu Casanovas	IDT-UAB	X
Coordinator	Carlos Monreal	S21sec	X

INDEX

EXECUTIVE SUMMARY

In D7.3 takes place the first evaluation of CAPER objectives and aims by the members of the Ethical Committee. They made several comments and valuable suggestions on the feasibility of the Caper Regulatory Model (CRM) presented in D7.1.

D7.3 constitutes an answer to the questions raised in their Reports: (i) What an ethical code consists of and where the regulatory power of ethics lays in the computer science field? (ii) Why are we contending that a code of ethics is not the adequate tool to regulate the technical deployment and practical management of CAPER? (iii) What is the nature of the CAPER Regulatory Model (CRM)? (iv) What do Privacy Impact Assessment (PIA) and Data Protection Impact Assessment (DPIA) mean? Are they adequate for CAPER? (v) Is there any convergence between a Web Services Platform such CAPER and the last developments of Privacy by Design? (vi) What are the most fruitful regulatory steps to be followed in the justice, security and freedom area to reach an agreement, and thus, to be effectively implemented in CAPER?

The answer to these questions has to be lined up with the fact that there is no specific data protection framework for the common foreign and security policy domain in the European Union yet. Several official documents and doctrinal volumes describe the situation as a “patchwork” of inconsistent regulations at the EU level. It is worthwhile not to forget that especially in the context of organized crime national law applies to LEAs’ activities and decisions. Thus, so far, EU Directives have had a deep but also limited impact. The new framework proposed in 2012 tries to uphold and back more regulatory powers for the EU control offices. But, still, this may happen or not. 2013 will be a transitional year, where these and other related issues will be discussed on political and legal basis in the European Parliement.

D7.3 displays also all the ethical and legal materials prepared by WP7 team to facilitate the evaluative work being performed by the Ethical Committee. This is the reason of the extended Annexes on ethicl codes and regulations.

Moreover, we show a connection between principles on Freedom, Security and Justice settled by Article 29 (Directive 95/46) Data Protection Working Party in 1997 and several converging formulations trecently rised in separate fields: (i) Linked Open Data Principles (T. Berners-Lee, 2006) (ii) Internet Identity Metasystem Layer: Laws of Identity (Kim Cameron, 2005), (iii) Privacy by Design Foundational Principles (Ann Cavoukian, 2006), (iv) Global Privacy Standard (Cavoukian, 2007), (v) LII Standards (Déclaration de Montreal, LAW.GOV Principles, The Hague Principlel, 2002-2012).

The WP activities related to the use of CAPER tools are divided into four successive stages: (i) profiling, (ii) storage, (iii) management, (iv) and transfer to third parties.

Focusing on this targeting, we are draw a first draft of Recommendations addressed to LEAs regarding the use of the tool. These recommendations are organized in tables to be distributed, acknowledged and discussed among them and the members of the Ethical Committee. The foundation for such recommendations lies on risks scenarios previously

defined — storage location and storing means; control of access; data retention and deletion; and security (backups, anonymizing, and response to breaches).

The general Data Protection principles that apply to LEAs activity are: (i) safeguarding fundamental rights; (ii) necessity in interfering with citizens' privacy; (iii) subsidiary and proportionality in those cases in which individual's right to privacy is being affected; (iv) accurate risk management on the basis of real risk, no hypothetical risk; (v) cost-effectiveness; (vi) bottom-up policy design strategy (design of governance structures); (vii) review ans sunset clauses (proposals in the area of freedom, security and justice will include obligations regarding annual reporting, and periodic and ad hoc reviews).

The draft of Recommendations constitutes a starting point for dialogue and the basis for a twofold purpose: (i) the set of issues (similar to Data Protection Impact Assessment) that will constitute the core of the ethical audit to be performed at the end of the project; (ii) the document containing Policies and Best Practices to be delivered as the final outcome of the CAPER regulatory Model (CRM).

The D73.1 output consists of: (i) a set of specific recommendations separately laid down for LEAs and partners; (ii) a set of specific rules to be taken into account and implemented into the CAPER technical building; (iii) a set of specific values and principles to be evaluated by the CAPER Ethical Committee; (iv) a theoretical model (CRM), that sets apart the networked and multi-levelled regulation which is needed in technological and organizational management.

1 INTRODUCTION

1.1 Aim of the Deliverable

The aim of this Deliverable is (i) presenting the ethical evaluation made by the CAPER Ethical Committee on the aims, objectives, procedures and effective solutions of CAPER, and (ii) based on this evaluation, providing a first set of recommendations to be followed by LEAs and members of the Consortium.

These recommendations based on an ethical and legal framework will constitute one of the main components of the final Caper Regulatory Model (CRM, see D7.1), to be released at the end of the Project (D7.8) as general guidelines for the management and administration of the platform, and for privacy and data protection policies.

The Ethical Committee is composed by Dr. Ugo Pagallo (Professor of Philosophy of Law at Torino University), Dr. Danièle Bourcier (Directeur de Recherche at CNRS-CERSA, Paris), Giovanni Sartor (Professor of Philosophy of Law at European University Institute of Florence), and Dr. John Zeleznikow (Professor of Information Systems at Victoria University). These four EC members, as EU experts on ICT Law and Ethics, discuss and eventually vote all the issues related with privacy, data protection and technical solutions. EC fifth member, Dr. Josep Monserrat (Associate Professor of Practical Philosophy at the University of Barcelona), expert in classical ethics and political philosophy, will also elaborate a report from the EU citizenship point of view. He will provide intellectual feedback acting as a third unrelated side, a “naïf” observer of the whole process.

The EC members are assisted by the members of WP7, who are responsible to facilitate their work and to implement their evaluation and reports into specific Recommendations for CAPER developments and the proper use of the tool. The duty of the EC consists of evaluating them and monitoring the development of the technical work. In order to frame and flesh out their first proposals, WP7 members put them three general questions to start with:

- Which are the "weak points" or the risks for citizens of the CAPER platform? National security vs. privacy.
- Is the intended CAPER Regulatory Model (CRM) feasible? Do you agree with the approach? What is missing? How can it be improved?
- Which would be the features of police behaviour, or the core of the principles they should follow regarding the use of data contained in the platform?

The Ethical Committee (EC) was provided with first-year materials (CAPER Scientific Memory) and the CAPER Deliverables on the subject; especially D7.1 (Regulatory and Ethical Framework) and WP2-Architecture Modeling. In the next future, as the CAPER Regulatory Model (CRM) develops, the EC will discuss particular solutions to the specific problems pointed out by LEAs, and will look after the audit and monitoring tasks regarding LEAs and CAPER members (D7.4).

This Deliverable is structured as follows. In Section 2, the reports of the Ethical Committee are exposed. In Section 3, we answer the questions they raised and we link the content of their comments to the state of the art for legal informatics, codes of ethics and governance. In Section 4, we set the European legal framework for Data Protection, Organized Crime and Terrorism. In Section 5, we discuss critical scenarios and specific problems for CAPER. As a result, two specific set of recommendations concerning data storage, management, security and privacy are eventually drafted: (i) addressed to researchers (ii) and addressed to LEAs. In a way, these recommendations are similar to the content of what it is known as Privacy Impact Assessment (PIA) and Data Protection Impact Assessment (DPIA) documents. However, we will show the difference between CRM, Ethical Codes and PIAs/DPIAs. The resulting Recommendations constitute a first body of regulations to be complied with by technical partners and LEAs in CAPER. Nevertheless, this body is a first draft, to be worked out, discussed and amended by the Ethical Committee, and to be refined in forthcoming Deliverables. Relevant documents and regulations are reproduced in the Annexes.

2 FIRST EVALUATION BY THE CAPER ETHICAL COMMITTEE: REMARKS ON THE ETHICAL CHALLENGES OF CRM (CAPER REGULATORY MODEL)

2.1 Report by Ugo Pagallo (University of Torino, Italy)[1]

2.1.1. Ethical Issues of CAPER

The aim of CAPER is essentially to set up a platform for LEAs to detect and prevent organized crime. Special attention is drawn to the concept of "security by design" and moreover, in accordance with art. 19(2) of the proposal for the police and criminal justice data protection directive, on the principle of privacy by design (and by default). This latter approach raises a number of ethical issues when the purpose is to prevent alleged harm-generating behavior from occurring through the use of self-enforcement technologies. However, so far, this is not the case of CRM since the model insists on both the role of social dialogue and the continuum of different regulatory instruments, to strike a balance between individual privacy and national security. As a result, let me dwell here on a further aim design may have, namely to decrease the impact of harmful behavior through the use of security measures.

2.1.2 The problem of personal data

This stricter approach to design mechanisms suggests that developers of information systems do not have to determine whether the processing of personal data is legitimate or what kind of data should be conceived of as personal. This does not mean, of course, that CRM should be considered as a value-free model. Suffice it to mention two aspects of the problem.

First, the focus is on the functional efficiency, robustness, reliability, and usability of the design project, through the use of prototypes, internal checks among the design team, user tests in controlled environments, surveys, interviews, etc. On this basis, we can prevent multiplying conflicts of values with their divergent interpretations through design choices, because these choices mostly concern the technical meticulousness of the project, rather than different political values and the autonomous decisions of individuals. Yet, the project has to strike a sometimes-difficult balance between, say, the efficacy of the information system and the fact that users, e.g. police officers, may find such mechanism too onerous.

Secondly, the continuum of regulatory instruments, such as hard and soft law, political decisions and ethics, makes it likely that some design choices shall be taken in order to implement the legal framework. Although the inclusion of values can draw on methods similar to those applied to other design criteria, such as functional efficiency and usability of the information system, a directive, rather than provisions of a stricter regulation, will define the EU legal framework. Consequently, in addition to the discretionary powers that Member

[1] Ugo Pagallo is Full Professor in Philosophy of Law at the Faculty of Law, University of Turin, European expert on technology, privacy and data protection law.

States can exert in the field, we should take into account the role of codes of conduct, best practices, and recommendations for the use of the platform. It follows that explicit regulation and even the sometimes-detailed guidance of legal doctrine help us overcome a relevant, but incomplete set of critical issues. Consider the connection between “privacy by design” and “security by design” which casts light on a number of open questions, such as: (i) striking a balance between individual privacy and national security, (ii) the feasibility of the CRM proposal, (iii) and Principles that police behavior should follow.

2.1.3 The balance between privacy and national security

As to the balance between the individual right to privacy and national security, provisions of the new legal framework are congruous with the basic safeguards of the system and the principles developed by both the Court of Justice of the UE and the European Court of Human Rights. In light of this latter case-law, for example, consider the principle of what is “necessary” pursuant to Article 8 of the ECHR in *Gillow vs. UK* from 24 November 1986, § 55; as well as in *Leander vs. Sweden* from 26 March 1987, § 59. Likewise, consider the principle of “predictability” in *Olsson vs. Sweden* from 24 March 1988, and the indispensable balance between what is necessary in a democratic society in the interests of national security and people’s right to respect for their private life (*Klass* et al. *vs. Germany*, 6 September 1978, § 59).

In the case of CRM, however, further attention should be paid to the three goals that are envisaged by the model, in connection with its four major components, namely data harvesting, analysis, semantic storage & retrieval, and access control. Such goals concern data mining components, a quick and robust import of data types from multiple data sources, and the progressively increasing detection capabilities of the system. Although such goals look appropriate and even necessary, they may raise a set of challenges and threats, as it occurs with techniques of individual profiling and how to manage cases of false positives. CRM can benefit from the remarks of Ann Cavoukian and Jeff Jones in *Privacy by Design in the Age of Big Data* (8 June 2012). Admittedly, some of their recommendations on the engineering of a next-generation sensemaking system do not fit our framework, e.g. false negative favoring methods and advanced analytics over cryptographically altered data. Yet, I reckon that some of their suggestions should be taken into account, such as the self-correcting false positives-approach, so that “with every new data point presented, prior assertions are re-evaluated to ensure they are still correct, and if no longer correct, these earlier assumptions can often be repaired – in real time” (op. cit., § 6 of the exemplar).

2.1.4 The feasibility of CRM

As to the feasibility of CRM, see supra 2.1.2 (ii), we should distinguish two different kinds of issues. The first set deals with the technical difficulty of applying to a machine concepts traditionally employed by lawyers, through the formalization of norms, rights, or duties: informational protection safeguards present highly context-dependent notions as personal data, security measures and data controllers, that raise a number of relevant problems when

reducing the informational complexity of a legal system where concepts and relations are subject to evolution. Since this is the kind of issues which CRM has in common with similar projects that aim to embed legal safeguards into technology, it seems more fruitful to dwell on what is specific to CRM. In light of the fifth commitment of the European Security Model, namely the involvement of the "social sector" that has to have a role to play in protection, CRM accordingly insists on the "cooperative behavior of citizens" and how much the "common resilience of governments, companies and citizens" is crucial to tackle the evolutionary context created by criminal threats. Aside from scant references to, say, a "community cloud," or "dialogue and communication with… social representatives and citizens [as] conditions for the overall system to work," the role of dialogue in the dynamics of CAPER, as illustrated in Fig. 8 of the framework for CRM (D7.1), seems still vague. Some further references or examples regarding the bottom-up implementations of the informational services regulations appear necessary.

As regards the principles that police behavior should follow, see supra 2.2. (iii), most of them have properly been stressed by CAPER's Ethical Committee doc at § 2 of the document on "cooperation in criminal matters" and, especially, at § 2.3 (conclusions). Here, let me focus on the aforementioned role of dialogue and the principle of accountability.

2.3.4 Dialogue and accountability

On one hand, both the introduction and conclusions concerning the framework for CRM put emphasis on dialogue, citizen cooperation, and the fact that "fighting organized gangs or illegitimated political violence is a social prerogative of the entire population under the rule of law." Accordingly, it seems appropriate that CAPER's ethical code should insist on the duty of enforcement powers, stemming from a legitimated authority, to strengthen and foster, whenever it is possible, such forms of dialogue and cooperation.

On the other hand, the principle of accountability is recalled at § 1.3.2 (IX) of the framework for CRM. Since CAPER's approach hinges on the principle of privacy by design and by default, intertwined with the aim to improve security by design, the principle of accountability may be further refined with the remarks of Cavoukian & Jones mentioned above at § 4: CAPER may, in other words, test its own system assumptions in light of these suggestions for a next-generation sensemaking system. Special attention should be drawn to the criteria of full attribution, data tethering, and tamper-resistant audit logs.

2.2 Report by John Zeleznikow (Victoria University, Australia)[2]

2.2.1 Which are the "weak points" or the risks for the citizens of the CAPER platform?

As Professor Pagallo notes the aim of CAPER is essentially to set up a platform for LEAs in order to detect and prevent organized crime. Special attention is drawn to the concept of “security by design” and moreover, in accordance with art. 19 (2) of the proposal for the police and criminal justice data protection directive, on the principle of privacy by design (and by default).

I do not agree with the statement that ‘This latter approach raises a number of ethical issues when the purpose is to prevent alleged harm-generating behavior from occurring through the use of self-enforcement technologies’. The Caper Regulatory Model more than adequately protects the right of citizens who either have been accused of endangering national security or even at risk of doing so. The model insists on both the role of social dialogue and the continuum of different regulatory instruments, to strike a balance between individual privacy and national security. If anything there is a bias towards the rights of individuals – a balance that does occur in neither Australia nor the United States.

2.2.2 Is the "CAPER Regulatory Model" being proposed feasible? Do I agree with the approach? What is missing? How can it be improved?

In developing a regulatory model from a set of guidelines, certain vital ethical decisions need to be made. For instance it is all very well to talk about individual rights vs national security, but ‘the proof of the pudding is in the eating’. The traditional European approach is to write down a set of guidelines. But it is very difficult to establish guidelines that are consistent, let alone complete.

Thus it might be wiser to use the British_USA_Australian common law tradition and develop a minimum set of guidelines with new cases providing for interpretation as needs be.

The idea of a Data Protection Impact Assessment is a good one. There is however no detail on how such a tool would be developed or evaluated. It would be an excellent idea to have such material incorporated into the documents.

2.2.3 Which are the "weak points" or the risks for the citizens of the CAPER platform?

As Professor Pagallo notes ‘the balance between the individual right to privacy and national security, provisions of the new legal framework are congruous with the basic safeguards of the system and the principles developed by both the Court of Justice of the UE and the

[2] John Zeleznikow is Full Professor of Information Systems and Director of the Laboratory of Decision Support and Dispute Management at the School of Management and Information Systems, Faculty of Business and Law, Victoria University (Melbourne, Australia).

European Court of Human Rights. In light of this latter case-law, for example, consider the principle of what is "necessary" pursuant to Article 8 of the ECHR in *Gillow vs. UK* from 24 November 1986, § 55; as well as in *Leander vs. Sweden* from 26 March 1987, § 59. Likewise, consider the principle of "predictability" in *Olsson vs. Sweden* from 24 March 1988, and the indispensable balance between what is necessary in a democratic society in the interests of national security and people's right to respect for their private life (*Klass* et al. *vs. Germany*, 6 September 1978, § 59).'

In the interests of national security, there is no alternative but to conduct individual profiling. The question then becomes as to how such profiling should be used. There is nothing wrong with more carefully investigating (within legal guidelines) the possible criminal actions of those being profiled. However when it comes to prosecuting such individuals, the full civil rights of these individuals must be protected. I believe the CAPER guidelines more than adequately meet these protections.

2.3 Report by Danièle Bourcier (CNRS, Paris, France)[3]

2.3.1 Which are the "weak points" or the risks for the citizens of the CAPER platform?

CAPER aims at setting up a platform for LEAs in order to detect and prevent organized crime. The concept of "security by design"4 is proposed as a means to govern and manage the infrastructures, softwares, contents or data that can be implied by the design of the system as a whole and integrated panoptican system. We have to welcome a project aiming at reinforcing security for citizens. However as a lawyer and member of ethical institutions on IT in France I have been already consulted on some of these issues. We all have been particularly aware by personal data and treatment of data such as profiling and any digital rights management systems (for example privacy but also copyright infringements). Some of these means can encapsulate some inaccurate data or improper interpretation of laws and principles (for example the "right to copy" was erased from most of the DRMs devices on e-commerce). The technical devices must be transparent and easily accessible due to the opaque way they are usually disseminated in a system. The rights of citizens to access and rectify one's own data must be designed in the device to achieve a real balance between security and data protection. In other words, security by design has to integrate privacy by design.

Then, in this project that deals particularly with fundamental rights, the proposed approach raises a number of ethical issues. The purpose is to prevent alleged dangerous behavior from occurring through the use of self-enforcement technologies.

[3] Danièle Bourcier is Member of the French National Committee of Science (COMETS-CNRS), and Member of the *Commission d'Ethique des Technologies de l'Information* (CERNA-ALLISTENE).
[4] In accordance with art. 19(2) of the proposal for the police and criminal justice data protection directive, on the principle of privacy by design (and by default).

The Caper Regulatory Model must integrate the right of all citizens to consider individual freedom as a fundamental value. This concerns not only the right of citizens who either have been accused of endangering national security or even at risk of doing so. It means that the impacts have to include the state of current freedoms and evaluate whether rights are affected by a too inclusive approach of the risk concerned. This is why we will have to observe the place of practical social dialogue and how these different regulatory instruments will be governed. Europeans have been pioneers in the field of data protection and we have to be aware of regulations where the protection has not provided an adequate level of protection specially when transfers of data can occur by definition.

2.3.2 Is the "CAPER Regulatory Model" being proposed feasible? Do I agree with the approach? What is missing? How can it be improved?

On the one hand, at this stage of the project, I consider that some precaution is needed without being able to prejudge the efficiency of what will be done to strike a balance between individual privacy and national security. The principle of precaution has already been used to evaluate automated systems applied to real life and can be used as a way to test the results of a system.

On the other hand, from a set of guidelines, it is feasible to design some technical constraints, as previous projects have achieved. It is of course a challenge but this ambitious project should include lawyers or legal engineers beyond parallel evaluation by an ethical committee, since it is not the same function. These legal engineers could implement inverse engineering to beta-test if the rules are relevant and correctly translated in the design. These experts can help not only ex post by evaluating but by suggesting ex ante.

It is not necessary to use Guidelines coming from Common law tradition: most of the countries in Europe have the Germano-continental tradition based on rules but also based on soft law (in other fields, see: Chart of environment in France, or Recommendation of scientific ethics by CCNE for example).

I agree with my colleague Pr. John Zeleznikow that Data Protection Impact Assessment is a good alternative. However, it has been already argued that no further detail is provided on ohw to perform a correct evaluation.

2.3.3 Which are the "weak points" or the risks for the citizens of the CAPER platform?

As Professor Pagallo notes in his legal references to European cases, there is a need to streake a balance when it comes to security and personal data protection. Nevertheless, it is harder to represent balancing interests than formal rules in a logical system. This is why rule based systems have been often considered as more adequate than case based systems to simulate a decision.

Note that there are two kinds of profiling: profiling or scoring calculated on data and algorithm built by the engineers of CAPER or profiles given by individuals on social networks. To build

profiles from statistics of data can be considered as useful for security risk assessment. However Directive 95/46/EC, and DIRECTIVE 2012/13/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 22 May 2012 on the right to information in criminal proceedings have clear statements on the limits of their use.

We have to emphasize on the second type of profiles, the risk to make inferences from social network data. It has been proven that many individuals use alias or avatars to open their own sites and play various roles using fake data. In the interest of national security, it it will be necessary to be aware of the game of Facebook users or other blogging platforms. The question then becomes how such profiling should be used. As regards profiling, in the field of Judiciary decision, the Directive maintains a similar position to the one of the French Regulation.5

I believe the CAPER guidelines must more adequately meet the precautionary principle concerning these two kinds of profiles: “profiles” given voluntarily by internet users and techniques of profiling. Even if the controller does not create profiles as such, processing activities can sometimes be considered ‘monitoring of behavior’ if they lead to decisions concerning a data subject or involve analyzing or predicting his or her personal preferences, behaviors and attitudes.

Finally, I would bring in the debate some comments of the Working Party 29 noting the fact that if the Commission has chosen to present a separate proposal for a Directive applicable to the area of police and criminal justice due to political constraints, “a high level of consistent data protection standards also applying to this area is all the more needed”.

The new legal framework should be in line with other international agreements, including Council of Europe Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data and its additional protocol. The same reasoning goes for the current specific rules for data processing in the former third pillar of the EU, for example in relation to EU agencies like Europol and Eurojust. The Working Party notes “the practical difficulties that may exist to propose a general overhaul of the current acquis, but at the same time believes the same high level of data protection should in the end be applicable to all

[5] *“Aucune décision de justice impliquant une appréciation sur le comportement d’une personne ne peut avoir pour fondement un traitement automatisé de données à caractère personnel destiné à évaluer certains aspects de sa personnalité.*

Aucune autre décision produisant des effets juridiques (perte d’un avantage)à l’égard d’une personne ne peut être prise sur le seul fondement d’un traitement automatisé de données destiné à définir le profil de l’intéressé ou à évaluer certains aspects de sa personnalité. *Ne sont pas regardées comme prises sur le seul fondement d’un traitement automatisé les décisions prises dans le cadre de la conclusion ou de l’exécution d’un contrat et pour lesquelles la personne concernée a été mise à même de présenter ses observations, ni celles satisfaisant les demandes de la personne concernée.* Loi n° 78-17 du 6 janvier 1978 relative à l'inform atique, aux fichiers et aux libertés. http://www.cnil.fr/?id=301 , Article 10 .

data processing in this area, including the EU bodies". The computer system must not go beyond what is necessary in order to achieve objectives of this Directive concerned.

2.4 Report by Giovanni Sartor (EUI, Florence)[6]

2.4.1 Which are the "weak points" or the risks for the citizens of the CAPER platform?

As my colleagues have remarked "The aim of CAPER is essentially to set up a platform for LEAs in order to detect and prevent organized crime". This is obviously a fully legitimate purpose, which justifes processing personal data, if proportionality is respected (CAPER effectively contributes to this purpose, better than the available less infringing alternatives, and without compressing to a comparatively unacceptable extent privacy and data protection). It seems to me that the platform is designed in such a way as to meet such requirements.

2.4.2 Is the "CAPER Regulatory Model" being proposed feasible? Do I agree with the approach? What is missing? How can it be improved?

I think that the CAPER regulatory model is very advanced and successfully captures the main normative requirements that underlie the management of personal data. I really appreciate this innovative and bold approach, which integrates suggestions coming from different disciplines.

One aspect which may be developed is how to deal with failures and provide for organizational learning. Failures can hardly be anticipated, but it would be good, I think, to have procedures for reporting privacy or security breaches or near-breaches, and the way to react by promptly intervening and mitigating failures. I will just address some more specific issues.

A significant issue which may emerge in connection with the use of CAPER is whether it distinguishes adequately data pertaining to different kinds of individuals. According to Art. 5 of the proposed directive on data processing by law enforcement authorities, we should distinguish between personal data of different categories of data subjects, such as:

(a) persons with regard to whom there are serious grounds for believing that they have committed or are about to commit a criminal offence;
(b) persons convicted of a criminal offence;
(c) victims of a criminal offence, or persons with regard to whom certain facts give reasons for believing that he or she could be the victim of a criminal offence;

[6] Giovanni Sartor is Professor of Legal informatics and Legal Theory at the European University Institute of Florence and at the University of Bologna, and President of the International Association for Artificial Intelligence and Law.

(e) third parties to the criminal offence, such as persons who might be called on to testify in investigations in connection with criminal offences or subsequent criminal proceedings, or a person who can provide information on criminal offences, or a contact or associate to one of the persons mentioned in (a) and (b); and
(e) persons who do not fall within any of the categories referred to above.

As different kinds of data subjects concern, so different types of information may require a different discipline. This involves in particular data concerning ethnical and racial background of data subjects and data concerning political opinion. How will CAPER address the possibility of extracting such information and the ensuing possibility of discrimination and violation of civil and political rights?

Another issue concerns the extent to which information in CAPER is to be communicated to all data subjects, taking into account the broad scope of data to be processed, and the fact that in many cases communicating this information may conflict with the purpose of the data collection. The CAPER model says that every data subject will be informed and will have the possibility to access his/her record. Will this always be the case?

For every datum in any database which refers to an identifiable person? What about data that identifies a single person only in combination with other data? Is the data subject to be communicated the entire cluster or only the result obtained on the basis of it? Moreover, the notion of what counts as personal data in the context of CAPER should be specified, namely, the different criteria for assuming that the data subject is identified or identifiable, and whether different degrees of identificability should be distinguished.

Finally, one further issue concerns controllers and processors of personal data. In the CAPER model will always LEAs be the controllers? Who will be a processor, and how the controller/processor relationship will be regulated? According to Art. 21 of the proposed directive Member States shall provide that the carrying out of processing by a processor must be governed by a legal act binding the processor to the controller and stipulating in particular that the processor shall act only on instructions from the controller, in particular, where the transfer of the personal data used is prohibited." What does CAPER propose in this regard?

2.4.2 Which are the "weak points" or the risks for the citizens of the CAPER platform?

I think that it is very difficult to regulate in advance the use that the police is going to make of the data stored in the platform. Obviously, the general principles of data protection should apply (in particular that collected for specified, explicit and legitimate purposes and eliminated, or anyway made inaccessible, when they are no longer needed for such purposes), and the police should be introduced to all layers of CAPER's regulatory model. Education I believe is an essential aspect of the project.

3 DISCUSSION: ETHICS, GOVERNANCE AND THE CAPER REGULATORY MODEL (CRM)

3.1 Introduction

Ethical Committee members have thoroughly commented on the general scope, aims, trends and main achievements of CAPER. They have broadly addressed a number of interesting issues, especially concerning the proposed CAPER Regulatory Model (CRM).

Ugo Pagallo points out the connection between “privacy by design” and “security by design” deepening into the answer to a number of open questions, such as: (i) striking a balance between individual privacy and national security, (ii) the feasibility of the CRM proposal, (iii) and Principles that police behavior should follow. This kind of multi-leveled cross-regulatory balance is also present in his recent work on law, robots and technology (Pagallo, 2012a; 2012b). He is suggesting a reevaluation of Privacy by Design, to be applied to the four major components of CRM: data harvesting, analysis, semantic storage & retrieval, and access control. Especially techniques of individual profiling and how to manage cases of false positives should be addressed in the construction of the platform.

John Zeleznikow suggests the elaboration of a Privacy Impact Assessment document (PIA) to monitor the development and management of the CAPER platform. In the common law tradition, he splits up legal and ethical issues —such as fairness, e.g. (Zeleznikow, 2012)— to harness the whole process. He notices a bias towards the rights of individuals in security matters. Danièle Bourcier retorts that in the European context personal data protection applies even in security scenarios according to the work of Working Party art. 29 and the consistent provisions of the Data Protection Directives. Profiling constitutes a problem, and Governance by design in cloud computing information networks implies the strict compliance of these principles (Bourcier and de Filippi, 2012). Giovanni Sartor’s report bridges the two perspectives. He agrees with Ugo Pagallo’s comment about the difficult balance between the protection of civil rights and that LEAs may find such mechanism too onerous: unrealistic pretensions to regulate in advance the use that the police is going to make of the data stored in the platform are helping neither to protect EU citizens nor to facilitating and improving police investigative tasks. However, the content of the boundaries set up by European legal rules regarding personal privacy has to be implemented into the CAPER design: procedures for reporting privacy breaches and repairing failures of the system must be faced and embedded into computing systems (Sartor, 2012).

National and European security constitutes certainly an exception for the application of data protection policies. Art 5 of the Madrid Joint Declaration on International Standards on the Protection of Personal Data and Privacy states:

States may restrict the scope of the provisions laid down in sections laid down in section 7 to 10 and 16 to 18 of this document, when necessary in a democratic society in the interests of national security, public safety, for the protection of public health, or for the protection of the rights and freedoms of others. Such restrictions should be expressly provided by national legislation, establishing appropriate guarantees and limits meant to preserve the rights of the data subjects, safety, for the protection of public health, or for the protection of the rights and freedoms of others.

All EU Directives on Privacy and Data Protection contain similar restrictions at the general level. However, as recalled by D. Bourcier's Report, there is a *non-regression principle* on freedom and human rights even in the Directives concerning criminal matters.[7] Protections were raised up since the beginning: "New technical means for data processing may only be introduced if all reasonable measures have been taken to ensure that their use complies with the spirit of existing data protection legislation".[8]

The European Court of Human Rights consistently holds a restrictive interpretation on Art 8 of the European Convention on Human Rights.[9] Safeguards and the meaning of "interference by a public authority" have been refined many times, as shown by the CJUE and ECtHR rulings recalled by Ugo Pagallo.[10] We could add, because of its significant consequences in data storage policies, *Marper*.[11] The Impact Assessment Document (IAD) of the proposed new Directive on Data Protection[12] mentions an extended record of rulings towards this direction, but it recognizes at the same time increasing difficulties in the area of justice, judicial and police cooperation due to the lack of harmonization among national legislations and the limited scope of the present Framework Decision regulating the processing of genetic data for the purposes of a criminal investigation or a judicial procedure.[13]

Difficulties for police authorities created by a variable and complex legal environment A police authority in one Member State (country A) is dealing with an

[7] Cfr. Art 10 of the recent Directive 2012/13/EU of the European Parliament and of the Council of 22 May 2012 on the right to information in criminal proceedings. "Nothing in this Directive shall be construed as limiting or derogating from any of the rights or procedural safeguards that are ensured under the Charter, the ECHR, other relevant provisions of international law or the law of any Member State which provides a higher level of protection".

[8] Principle 1.2 of the Recommendation No. R (87) 15 of the Committee of Ministers to Member States Regulating the Use of Personal Data in The Police Sector (Adopted by the Committee of Ministers on 17 September 1987 at the 410th meeting of the Ministers' Deputies).

[9] Article 8 – "Right to respect for private and family life. 1. Everyone has the right to respect for his private and family life, his home and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others".

[10] Among many others, *Gillow vs. UK* from 24 November 1986, § 55; *Leander vs. Sweden* from 26 March 1987, § 59; *Olsson vs. Sweden* from 24 March 1988); *Klass* et al. *vs. Germany*, 6 September 1978, § 59.

[11] ECtHR, *S. and Marper* v. *The United Kingdom*, Judgment of 4 December 2008. Cfr. Paul de Hert (2012, 57-58) commenting on *Marper:* "In conclusion, the Court finds that the blanket and indiscriminate nature of the powers of retention of the fingerprints, cellular samples and DNA profiles of persons suspected but not convicted of offences, as applied in the case of the present applicants, fails to strike a fair balance between the competing public and private interests and that the respondent State has overstepped any acceptable margin of appreciation in this regard. Accordingly, the retention at issue constitutes a disproportionate interference with the applicants' right to respect for private life and cannot be regarded as necessary in a democratic society. *This conclusion obviates the need for the Court to consider the applicants' criticism regarding the adequacy of certain particular safeguards, such as too broad an access to the personal data concerned and insufficient protection against the misuse or abuse of such data* [Italics added by de Hert]*."*

[12] Impact Assessment accompanying the proposed Directive and Regulations, Comission Staff WP Imact Assessment, Brussels, 25.1.2012 SEC(2012) 72 final.

[13] See the criticisms at the Framework Decision (2008) in pp. 32 and ff.

investigation related to cross-border trafficking of human beings. The nature of the case implies that information, including personal data of suspects, is required from two other Member States (country B and country C). When processing the data related to the above investigation, the police authorities in country A have to apply different data protection rules for different aspects of the file related to the investigation, depending on whether the data come from their own Member State or have been received from country B or C.

This means that, for example, different rules may apply to the further transmission of data related to the investigation – which may not be easily separated/distinguished depending on their origin - to other non-police authorities (i.e., immigration or asylum authorities) or in relation to the information that can be provided to the individuals concerned.[14]

Especially in this area of criminal justice and organized crime, all the Ethical Committee reports lead to the conclusion that police cooperation is a priority for the EU. Thus, ethical and legal issues are deeply intertwined. There is no clear-cut line between ethical and legal topics, because they are embedded into EU principles, best practices and policies.

It is our contention that to apply those to CAPER there are two assumptions to be made: (i) the need for a theoretical model to articulate in a concrete way the different principles, rules and practices at stake; (ii) the recognition of the regulatory power of ethics as a rational means to thinking about law, citizenship, justice and security, and linking all the relevant aspects into a single, specific and feasible model. Dialogue is crucial to reach understanding and willingness from all the stakeholders.

Therefore, our answer to the EC considerations will face these questions:

- What an ethical code consists of and where the regulatory power of ethics lays in the computer science field?
- Why are we contending that a code of ethics is not the adequate tool to regulate the technical deployment and practical management of CAPER?
- What is the nature of what we have called in D7.1 the CAPER Regulatory Model (CRM)?
- What do Privacy Impact Assessment (PIA) and Data Protection Impact Assessment (DPIA) mean? Are they adequate for CAPER?
- Is there any convergence between a Web Services Platform such CAPER and the last developments of Privacy by Design (as suggested by Ugo Pagallo's report)?
- What are the most fruitful regulatory steps to be followed in the justice, security and freedom area to reach an agreement, and thus, to be effectively implemented in CAPER?

3.2 Ethics and Computer Ethics

Morals are one of the fundamental dimensions of human being's behavior. Very broadly, Ethics, as a philosophical discipline, covers all reflections, writings and thesis sustained over the centuries on matters such as power, justice, freedom and law in human civilizations by intellectuals, scientists and philosophers.

[14] Impact Assessment, op. cit. p. 35.

In the last sixty years, after the II World War, accordingly with the new problems posed by the developments of nuclear weapons, the raising of information theory, Artificial Intelligence, and the impact of technology into everyday life, the ethical and professional aspect of computer science emerged. Like Oppenheimer, Norbert Wiener was deeply concerned by the strength and precision of technological tools. He wrote *The Human Use Of Human Beings: Cybernetics And Society* (1950), where he divided the devils facing us in two kinds: (i) the "Manichean Devil", determined on victory using any trick or dissimulation to obtain it, and (ii) the "Augustinian devil", characterized by chance and disorder (as nature), but who cannot change the rules (Galison, 1994).

Wiener pointed out the three elements bounding the ethical space in computing: nature, rationality, and values. Contemporary philosophy of science contends that "a rational moral rule has exactly the same structure than a technological rule, in the sense that both lie on scientific laws and explicit evaluations" (Bunge, 1996). Moral rules are conceived, thus, as behavioural rules derived from scientific statements and judgements of value.

There is then a regulatory aspect of Ethics than can be rooted on truth and professional behaviour in applied domains. *Information Ethics*, *Computer Ethics* and *Cyberethics* are names usually used to term this field. Norms, rules, and values are seen as tools with the scope to reach better professional and scientific achievements. Similarly, *Ethical Codes*, *Codes of Ethics*, *Corporate Codes*, *Codes of Behaviour* and *Best Practices* are different denominations to design how norms, rules and values are tied together as standards for a certain field. This can be done from a corporate or practical point of view —as most professional codes do— or from a more reflective and philosophical perspective. Luciano Floridi, e.g., launched the notion of "re-ontologization" of computer ethics: "computer and ICTs are ontologising devices because they engineer environments that the user is then enabled to enter through (possibly friendly) gateways" (Floridi, 2007, 185).This idea —"a system designer is the demiurge of the artefacts he produces"— tries to capture the making and managing of computing, and is acting as a blueprint or hallmark in the ethics of design[15]:

We will take advantage of it as well, but John Zeleznikow put in a quite straightforward way the task we have to carry out in regulatory matters: '*the proof of the pudding is in the eating*'.

What an ethical code consists of? Where the regulatory power of ethics lays in the computer science field? And why are we contending that a code of ethics is not the adequate tool to regulate the technical deployment and practical management of CAPER?

3.2.1 Ethical Codes

An Ethical Code is an ordered set of principles, values and rules, aiming at serving as guidelines for the individual, social and professional behaviour in a company, corporation, organization or human institution. Thus, ethical codes are moral and formal guidelines adopted to regulate behavioral patterns into organizations, companies or institutions.

[15] "Nowadays, a system designer must have a deep understanding not only of the social and legal implications of what he is designing but also of the ethical nature of the systems he is conceptualising. These artefacts not only behave autonomously in their environments, embedding themselves into the functional tissue or our society but also 're-ontologise' part of our social environment, shaping new spaces in which people operate." (Turilli, 2007, 60-61)

There is an extensive literature on their origins and development in the 20c16. McDonald (2009: 345-46) summarizes the most common motivations for the adoption of codes of ethics into seven reasons:

(1) Ensuring legal compliance and other statutory requirements;

(2) providing a guide for behaviour and formalised expectations;

(3) protecting and enhancing organisational reputation;

(4) ensuring employee, management and supplier compliance and minimising risk;

(5) ensuring consistency across global networks;

(6) creating and maintaining trust and confidence with stakeholders; and

(7) communicating principles and commitments to stakeholders.

Perhaps the most extended application of ethical codes is being produced in corporations and business, as bases for good governance. Conflicts of interest, professional misconduct and members' organizational complaints are filtered also through Ethical Committees that are pragmatically oriented to solve them without the resort of legal suits. Thus, they act as suit-avoiding devices.

Bondy et al. (2006), as quoted by McDonald as well (2009), identify four distinctive styles of codes in the business field:

(1) Stipulative codes which used words such as "shall", "will" and "required". Stipulative codes also frequently included sanctions or threats for non-compliance.

(2) Commitment-based codes that indicated a corporation's intention to engage in corporate social responsibility and to provide some indication of how this engagement will occur.

(3) Principles-based codes which indicate a corporation's over-arching philosophy and the principles that underpin the organisation's approach to managing ethical behaviour.

(4) Information-based codes, these codes are largely informative and are comprised of information on what has already been done by the corporation in relation to its corporate responsibilities. The underlying qualitative characteristics of a code have been identified as; specificity, publicity, clarity, revisability, and enforceability.

[16] Cfr. Farrell et al. (2002): Bondy et al. (2006); McDonald (2009).

Other taxonomies include inspirational and prescriptive types (Cressy and More, 1983), and allodial or decretal types, based on the presence or absence of operational definitions (Farrell et al. 2002). Public scrutiny and openness are preconditions for their implementation.

Other fields where they have been successfully applied are medicine, biology and research implying ethical issues (such as genetics). In these fields, codes of ethics applied to human research are also implemented by Ethical Committees that "are more regulatory authorities than simple ethical reviews" (McGiness, 2008, 699).

Evidence suggests that the adoption of codes is more relevant in some industries than others. There is a relationship between the adoption of ethical codes and industry type: "Industries such as the computer, electronic, scientific and photographic sectors that are involved with high-precision products, as well as industries mining crude oil, petroleum and natural resources, are more inclined to have a formal written code of ethics" (McDonald, 2009, 359). In technology, ethical codes have been developed since the eighties to regulate professional and research behavior, alike.

Organizations such IEEE17 and ATM18 have laid down ethical regulations. There are some recent attempts to unify (market) business and ITC professional ethics. Payne and Landry (2006) base the proposal on seven basic principles: consistency, respect for individuals, autonomy, integrity, justice, utility and competence (Table 1).

Basic Professional Ethical Principle	ICCP Code	ACM Code	AITP Code	Uniform IT Professional Principle
Consistency Respect for individuals Autonomy	ICCP Prin. 2: The IT professional will maintain a confidential relationship with people served ICCP Prin. 4: The IT professional will observe an ethical code	ACM Prin. 3: ACM members should accept assignments for which there is expectation of achieving reasonable results and perform his assignments in a professional way ACM Prin. 4: ACM members should act with professional responsibility	AITP Prin. 2: AITP members should uphold the ideals of the AITP, work with each other and treat others with honesty and respect AITP Prin. 4: AITP members should uphold educational institution's moral principles AITP Prin. 6: AITP members should respect their countries and act accordingly; AITP members should uphold the ideals of the AITP, work with each other and treat others with honesty and respect	Treat constituents fairly, with uniformity in consistent situations, regarding safety, knowledge and good faith Assure freedom of choice by providing information that is accurate, relevant and complete to all appropriate stakeholders
Integrity Justice	ICCP Prin. 2: The IT professional will maintain a confidential relationship with people served ICCP Prin. 4: The IT professional will observe an ethical code	ACM Prin. 1: ACM members should act with integrity	AITP Prin. 3: AITP members should disseminate knowledge about the development and understanding of information processing AITP Prin. 5: AITP members should guard the employers' interests and advise the employers wisely and honestly	Use good faith in decision making and assessment activities
Utility Competence	ICCP Prin. 1: The IT professional will embrace a high standard of skill and knowledge ICCP Prin. 3: The IT professional will recognize public reliance upon the standards of conduct and established practice	ACM Prin. 2: ACM members should strive to increase their competence and the competence and prestige of the profession ACM Prin. 5: ACM members should use specialized knowledge and skills for the advancement of human welfare	AITP Prin. 1: AITP members should promote management's understanding of information processing methods and procedures	Assess utility and competence of project and self in light of the social and individual needs and abilities of stakeholders and society

Table 1. A uniform code of ethics for business and IT professionals.Source: Payne and Landry (2006, 84).

[17] http://www.ieee.org/about/corporate/governance/p7-8.html
[18] http://www.acm.org/about/code-of-ethics

In this comparative table, the first three principles (consistency, respect for individuals, autonomy) are conceived as a sort of Kantian "golden rule"; a second set of principles (integrity and justice) are grouped reflecting basic principles of good faith and fairness; finally, utility and competence fit together from a standpoint of pragmatism, "sice social utility is served by competence" (ibid. 2006, 84).

This is an interesting attempt to assemble the content of ethical codes. As we will show below, The Ethical Code of the Computer Ethics Institute19, the Code of Ethics for the Information Society (UNESCO)20, the ISSA Code of Ethics21, are useful documents as well. But it is worthwhile to notice that universal principles always require complementary tools to be implemented for solving specific cases. Therefore, when launched into organizations, they usually come with procedurals rules for conflict resolution among the members. Again, Ethical Committees are compelled to behave as regulatory authorities, with a high degree of discretionary power in their decisions.

3.2.1.1 *Ten Commandments for Computer Ethics*

The Computer Ethics Institute launched these general principles, mimicking the biblical commands:

1. Thou Shalt Not Use A Computer To Harm Other People.
2. Thou Shalt Not Interfere With Other People's Computer Work.
3. Thou Shalt Not Snoop Around In Other People's Computer Files.
4. Thou Shalt Not Use A Computer To Steal.
5. Thou Shalt Not Use A Computer To Bear False Witness.
6. Thou Shalt Not Copy Or Use Proprietary Software For Which You have Not Paid.
7. Thou Shalt Not Use Other People's Computer Resources Without Authorization Or Proper Compensation.
8. Thou Shalt Not Appropriate Other People's Intellectual Output.
9. Thou Shalt Think About The Social Consequences Of The Program You Are Writing Or The System You Are Designing.
10. Thou Shalt Always Use A Computer In Ways That Insure Consideration And Respect For Your Fellow Humans.

3.2.1.2 *(ISC)² Certification Behavior*

Some Codes are focused on complaint procedures for members of the organization and show (willingly) a lack of provisory rules, leaning instead on procedural ways. E.g. On (ISC)² certification behavior, a quite detail procedural affidavit is foreseen and advanced for all members[22], but the Ethical Code consists only of four very broad commands:

> **Code**
> All information systems security professionals who are certified by (ISC)² recognize that

[19] http://computerethicsinstitute.org/publications/tencommandments.html
[20] See Annex 9.1.2, below, http://unesdoc.unesco.org/images/0021/002126/212696e.pdf See for comments, Cappurro and Britz (2010).
[21] https://www.isc2.org/ethics/default.aspx ; see below, 3.2.13.
[22] See Annex 9.1.3, below, Ethics Complaint Procedures.

such certification is a privilege that must be both earned and maintained. In support of this principle, all (ISC)² members are required to commit to fully support this Code of Ethics (the "Code"). (ISC)² members who intentionally or knowingly violate any provision of the Code will be subject to action by a peer review panel, which may result in the revocation of certification. (ISC)² members are obligated to follow the ethics complaint procedure upon observing any action by an (ISC)2 member that breach the Code. Failure to do so may be considered a breach of the Code pursuant to Canon IV.

There are only four mandatory canons in the Code. By necessity, such high-level guidance is not intended to be a substitute for the ethical judgment of the professional.

Code of Ethics Preamble:
Safety of the commonwealth, duty to our principals, and to each other requires that we adhere, and be seen to adhere, to the highest ethical standards of behavior.
Therefore, strict adherence to this Code is a condition of certification.

Code of Ethics Canons:

- Protect society, the commonwealth, and the infrastructure.
- Act honorably, honestly, justly, responsibly, and legally.
- Provide diligent and competent service to principals.
- Advance and protect the profession

3.2.1.3 ISSA Code of Ethics

The ISSA policies also contain some procedures (including mediation) to conduct hearings and to present complaints of professional ethical misconduct[23], but the standards to be implemented are a recall of universal principles[24]:

The primary goal of the Information Systems Security Association, Inc. (ISSA) is to promote practices that will ensure the confidentiality, integrity, and availability of organizational information resources. To achieve this goal, members of the Association must reflect the highest standards of ethical conduct. Therefore, ISSA has established the following Code of Ethics and requires its observance as a prerequisite for continued membership and affiliation with the Association.

As an ISSA member, guest and/or applicant for membership, I have in the past and will in the future:

- Perform all professional activities and duties in accordance with all applicable laws and the highest ethical principles;
- Promote generally accepted information security current best practices and standards;
- Maintain appropriate confidentiality of proprietary or otherwise sensitive information encountered in the course of professional activities;
- Discharge professional responsibilities with diligence and honesty;

[23] See Annex 9.1.4, below.
[24] Cfr. "Ethics and Security", ISSA Ethics Committee Presentation, www.**issa**.org/resource/resmgr/pdf/**ethicscommittee**overviewprese.ppt

- Refrain from any activities which might constitute a conflict of interest or otherwise damage the reputation ofor is detrimental toemployers, the information security profession, or the Association; and
- Not intentionally injure or impugn the professional reputation or practice of colleagues, clients, or employers.

3.2.2 Security Ethics

Ethical Codes have attracted a lot of attention either from the security private sector or the public one.[25] There have been several attempts to reach a general consensus to formulate a general security code of conduct.[26] However, consensus is not common on this topic (Greenwald et al. 2008). It has been pointed out that information ethics cannot cover all the issues which are present in information security ethics. Experts use to agree that the difference lies on the assumptions taken for granted:

> Information security ethics involves a paradigm shift away from the standard ethical paradigm of computer science as found in our canonical professional societies like ACM and IEEE. The dominant paradigm in computer science ethics does not assume a *malicious* universe; instead it assumes the standard scientific paradigm notion of an *impartially disinterested* universe; *nota bene* that the idea of teleology in most scientific paradigms comes as close as science ever does to heresy (the sign of a Kuhnian paradigm shift of course). But in the information security field we certainly must assume a malicious universe not only due to the adversarial nature of the people involved, but also due to the existence of proxies (malware) that run on the behalf of human adversaries (or even taking on a "life of their own")" (Ibid. Snow, in Greenwald et al. 2008, 75)

Scenarios are even more complex in the public sector.[27] Especially in justice and police cooperation issues, national policies are at stake and not only protective roles or professional

[25] Public sector has some differential features. McDonald (2009) cautions quoting Doig and Wilson (1998) that "the public sector must realise that it cannot look solely to formal codes to revive and sustain public sector values. Despite the proliferation of codes there are those that are somewhat cynical of the motivations underpinning their introduction and use. For example, there is the danger of codes being seen as something more than they really are, and being used primarily to deflect criticism and reduce the demand for external regulation".

[26] Cfr. the Preamble of GAIP. v. 3. From the ISSA (Information Systems Security Associations): "GAISP – the Generally Accepted Information Security Principles project – has been formed to address the fact that the practice of Information Security – IS is now at a crossroads. While IS professionals have made strides towards staying a step ahead of rapidly evolving threats, in moving from reactive to proactive practices the professional community has grown in a fragmented manner with little cohesive organization. This is hardly surprising, given that security has historically been an afterthought in product development, creating a perpetual catch-up mentality that has stunted the growth of a solid organizational foundation and framework for guidance. Still much in its infancy stage, the information security industry is now searching for cohesion, organization, and for acceptance of the need to be an integral part of technology management".

[27] Although the public space has some differential features. McDonald (2009) cautions quoting Doig and Wilson (1998) that "the public sector must realise that it cannot look solely to formal codes to revive and sustain public sector values. Despite the proliferation of codes there are those that are somewhat cynical of the motivations underpinning their introduction and use. For example, there is the

duties. The situation of vulnerablity in Europe often encounters the boundaries of nation-state as a limitation for cooperation policies and initiatives.[28]

Twenty-five years ago, Michel Davies warned against the formal or loose application of ethical codes or best practices to the police, without any participation or inner insight of the problems police has to face:

> A *code of ethics* is a formal statement of a group's ethics, whether descriptions of a preexisting practice (like a dictionary's definition) or a formula creating the practice (like a definition in a contract). We may distinguish three distinct kinds of code: statements of ideal ("credos" or "aspirations"); statements of principle ("guidelines" or "ethical considerations"); and statements of requirement ("codes of conduct," "mandatory rules," or simply "duties"). While I would prefer to reserve "code of ethics" for the last of these, I cannot do that here without risking confusion. Not only has "code of ethics" been used indiscriminately for codes of each kind, it has also been used for codes placing statements of one kind next to statements of another, without any suggestion that, for example, some are requirements while others are mere ideals. Codes of police ethics are at least as likely to do this as those of other professions. The consequences are not good. (Davies, 1991, 14)

We see how this discussion reflects and mirror the tensions between civil rights and security already tackled in privacy and personal data protection fields. The need for transnational governance and “transgovernmental networks” (Hollis, 2010), and the prospective vision of “ethical proactive threat research”(Aycock and Sullins, 2010) are counterbalanced by the political and legal requirements of stopping torture (Dittrich et al. 2011) and warnings against the suspension of due process in terrorist cases (Crank and Gregor, 2005).

To be effective, a code of ethics should offer open possibilities of being interpreted and acted. Davies (2001) argues that there are three myths about information ethics that are mutually reinforcing: a) that the first codes of engineering ethics put loyalty to client or employer ahead of the public interest; b) that engineering codes of ethics should be mere (moral) guides rather than (legalistic) rules; and c) that codes of engineering ethics are too vague to provide much guidance.

However, this is not the main trend in the field, for in most ethical codes simplicity and clarity are preferred over more complex hermeneutics. Formulations within the military, e.g., show the same performative self-conscious behavior than the examples we mentioned above.

---

danger of codes being seen as something more than they really are, and being used primarily to deflect criticism and reduce the demand for external regulation”.

[28] “The energy debacles in Ukraine, the terrorist bombings in London and the forest fires in Portugal have highlighted Europe’s interconnectedness and vulnerability. Largely in reaction to these and several other crises, the EU has developed a crisis management capacity to prevent, prepare for and respond to natural and manmade disasters in a functionally interdependent Europe. The MIC, the Joint Situation Centre (SitCen) and the EU’s Judicial Cooperation Unit (EUROJUST) represent just some initiatives that have been instigated in the last decade aimed at tackling a wide range of common threats. However, it is not just past events that have shaped this policy area. Whether it is the result of an expanding democratic deficit, maintaining regulatory control or guarding national sovereignty, *the effectiveness of EU integration in crisis management is restricted by the resistance of member states to concede political authority to the EU*” [emphasis added] (Hollis, 2010).

See, e.g., the following conditions for ethical codes addressed to US Intelligence officers (Snow and Brooks, 2009, 31):

- The code should be aspirational, not proscriptive. That is, it should outline behaviors to aspire to and not get into specific details of do's and don'ts.
- It should not be viewed as regulation or law, but as guidelines for making difficult decisions.
- It should be a set of short, easily understood sentences (for example, the Ten Commandments are not verbose).
- The statements must address at least the issues of lawfulness, transparency, accountability, truthfulness, examining consequences of planned actions, and protection of innocent individuals.
- It should be unclassified and explicitly made available to the public.

There is no clear solution for the dilemma simplicity (i.e. clarity, direct meaning) vs. complexity (i.e. open texture, interpretation). What would make sense to do to find an exit from the maze?

3.2.3 Ethical governance: a dynamic space

Especially in the area of security, justice and freedom, we think that we can preserve simplicity only if moral standards are embedded in another kind of political and legal principles, switching from the level of human (individual) interaction to a human-machine artificial interface in which technical protocols matter. In CAPER it is not the case to lay down a single ethical code (which seems more suitable for professional or organizational fields with a broader scope), but to select relevant building blocks for the good governance of the system.

CAPER is a platform for web services, which brings together and it allows LEAs of different kinds and different national states to crawl the web and store, link and exchange sensitive, personal and private data. This is a kernel, a cross-road of different values, opinions, practices and interpretations. In this scenario, we think that moral standards should remain clung to the common legal system which, in addition to national legal ones, is a mixture of European legislation, international law, sentences and prominent legal doctrine. Even if it is not easy to navigate in such a sea, especially in this field, something is better than nothing.

This is the sense of the institutional strengthening model plotted on Fig. 1.

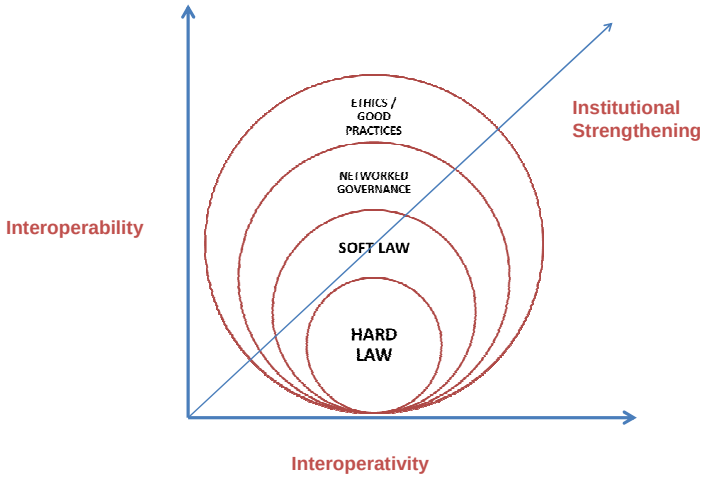

Fig. 1. Source: D7.1, Casanovas (2013, 29)

We developed this approach in WP7 D7.1 (1.3.1-1.3.2). “Institutional strengthening” points to the collective property that emerges of the process of implementing a model seeking a certain balance between the binding power of the rule of law and the dialogue among all the stakeholders, including the different polices, web service providers and citizens.

The only way to find a structure for the ethical building blocks is setting out a conceptual model anchored onto relevant judicial and legal rulings: hard law is what generates and fuels the conditions for creating and managing tools of governance, best practices and ethics. The model is built up taking elements from models representing different sectors (e.g. private: data governance; public: data protection), and legal and political arenas. It is conceptual in nature: it cannot be confused with the detailed recommendations for LEAs and researchers that will constitute its output. Common guidelines, best practices, are the rules to be followed by CAPER partners and LEAs to give an answer to practical problems (e.g. how long data can be stored in the platform?). CAPER Regulatory Model (CRM) is the theoretical model which is behind the recommendations, with three different dimensions and four vertex triggering several edges —types of regulations— and planes —perspectives:

I. Hard Law [Security, Data Governance, Data Protection]
II. Soft Law [Security, Data Protection, Privacy]
III. Networked Governance [Data Governance, Data protection, Privacy]
IV. Ethics and Best Practices [Security, Privacy, Data Governance]

As already shown in D7.1, in this design interoperability (or “system governance”) and *interoperativity* (a Neologism borrowed from Latin languages standing for “organizational governance”) are situated in the center of the volume created by the continuum I-IV and represented by the length, breadth and height of the CRM cube.

Thus, CRM tries to sum up and represent the dynamic dimension of what Jensen et al. (2009) have called “the dynamic bending of the moral space”: “The code comes alive in a heterogeneous materiality, travelling as a result of a wide range of translations, and granted an epistemological capability of influencing humans’ world-views and moral practices.” (ibid. 529). But to avoid being “a passive voice or a blueprint upon which organizational change is performed” (ibid. 530) there is not an ethical code what it is needed, but a more complex set

of regulations combining materials from all the relevant legal, moral, political and rational (argumentative) sources, and in which ethical values are embedded.

This is a *cultural and organizational perspective* which is common in the business context as well, because social responsibility "stems not from the mere existence of codes of ethics and conduct, but rather from the development of functional organizational cultures that have a strong ethical dimension (i.e. they are infused with ethical decision-making principles which underpin ethical leadership and followership behaviors)" (Wickham and O'Donohue, 2012). Therefore, the creation of an "ethical climate" is crucial and even more important than the representation of rules and principles: it refers to the extent to which perceptions, of what comprises ethically correct behaviour and how ethical issues should be handled, are shared across the organization (ibid.).

We do believe that CRM combines:

- Ethical imagination and design: comparative work between different architectural activities (Lloyd, 2009).
- Ethical intelligence: the resources and capabilities needed to develop an enduring commitment to ethical decision-making and conduct in the interests of the organization that goes beyond mere compliance with organizational codes (Wickham and Donohue, 2012).
- Organizational intelligence: (i) the capacity of individuals to sense, monitor and scan specific aspects of their environment; (ii) individuals being able to relate this information to the organization's operating norms; (iii) the ability of individuals to detect significant deviations from these norms; and (iv) the willingness of individuals to initiate corrective action when discrepancies are detected – either by adjusting strategy, and/or transforming the organization's norms (Albrecht, 2002, as quoted by Wickham and Donohue, 2012).
- Ethical governance: the role that ethical and political organizational infrastructure might play in establishing and maintaining policies and effective ethical decision-making processes and behaviours (Salminen, 2010).

3.3 Privacy Impact Assessments (PIAs), Privacy by Design (PbD), and Linked Open Data (LOD)

3.3.1 Impact Assessments (PIAs and DPIAs)

What do Privacy Impact Assessment (PIA) and Data Protection Impact Assessment (DPIA) mean? Are they adequate for CAPER?

We should clarify now the meaning of "Impact Assessment" workflows and documents. Broadly speaking, they consist of all sorts of studies, measurements and reflections about the social, ethical and legal effects and consequences of certain policies, regulations and practices.

From the past twenty years on it has become commonplace to apply "Impact Assessments" (IA) to privacy (Privacy Impact Assessments, PIAs), regulations (RIAs), surveillance (SIAs) and data protection (DPIAs). Implementing a PIA or a DPIA means a sort of monitoring audit

that goes along the process of creating, testing, reviewing and eventually enforcing a regulatory tool (including technological projects and economic planning). They have been adopted mainly to evaluate intended legislation and public policies (see an IA standard structure in Table 2).

> Central to better regulation at governmental level has been the use of RIA/IAs as an integral part of the policymaking process. Governments should intervene in markets only where there is clear market failure and where state intervention is the least costly solution. The purpose of RIA/IA is to assess and measure the costs and benefits for a range of options so as to ensure that market failure is addressed at least net cost or with the largest net benefit. The use of RIA/IA is intended to contribute to good governance and in turn improved economic performance. (Parker, 2012, 95)

1. *Statement of problem*. Is government intervention both necessary and desirable?
2. *Definition of alternative remedies*. These include different approaches, such as the use of economic incentives or voluntary approaches.
3. *Determination of physical effects of each alternative, including potential unintended consequences*. The net should be cast wide. Generally speaking, regulations or investments in many areas of public policy can have social, environmental and other implications that must be kept in mind.
4. *Estimation of benefits and costs of each alternative*. Benefits should be quantified and where possible monetised. Costs should be true opportunity costs not simply expenditures.
5. *Assessment of other economic impacts*, including effects on competition, effects on small firms, international trade implications.
6. *Identification of winners and losers*, those in the community who stand to gain and lose from each alternative and, if possible, the extent of their gains and losses.
7. *Communication with the interested public*, including the following activities: notification of intent to regulate, request for compliance costs and other data, public disclosure of regulatory proposals and supporting analysis, and consideration of and response to public comments.
8. *A clear choice of the preferred alternative*, plus a statement defending that choice.
9. *Provision of a plan for ex post analysis of regulatory outcomes*. It is important to establish a benchmark against which to measure performance. Planning is needed to ensure that procedures are in place for the collection of date to permit such benchmarking.

Table 2. Common Characteristics of Impact Assessments. Source: Parker (2012, 80)

PIAs have been currently adopted by Common Law countries like USA[29], Canada[30], UK[31], Australia[32], and New Zealand for the protection of civil (human) rights regarding personal data. David Wright et al. (2011) just established the state of the art of PIAs processes in these countries (adding Ireland and Hong Kong) in a EU 7F Project. Roger Clarke (2011) has furnished a detailed analysis of PIA guidance documents, and he advances some criteria to evaluate their quality.[33] The *Privacy Impact Assessment Handbook* (Office of the Privacy Commissioner of New Zealand)[34] defines a PIA as follows:

[29] Many USA organizations link PIAs with security issues, e.g. the Postal Service, http://about.usps.com/handbooks/as353/as353c3_008.htm

[30] http://www.priv.gc.ca/resource/fs-fi/02_05_d_33_e.asp

[31] http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/privacy_impact_assessment.aspx ; http://www.ico.gov.uk/upload/documents/pia_handbook_html_v2/files/PIAhandbookV2.pdf

[32] www.privacy.gov.au

[33] 1. Status of the Guidance Document 2. Discoverability of the Guidance Document 3. Applicability of the Guidance Document 4. Responsibility for the PIA 5. Timing of the PIA 6. Scope of the PIA (a) The Dimensions of Privacy (b) Stakeholders (c) Reference Points 7. Stakeholder Engagement 8. Orientation (a) Process compared to Product (b) Solutions compared to Problems 9. The PIA Process

> Privacy Impact Assessment (PIA) is a systematic process for evaluating a proposal in terms of its impact upon privacy. PIA helps an agency to:
> • identify the potential effects that a proposal may have upon individual privacy
> • examine how any detrimental effects upon privacy might be overcome
> • ensure that new projects comply with the information privacy principles.

The Australian *Privacy Impact Assessment Guide* states simply: "A PIA 'tells the story' of a project from a privacy perspective and helps to manage privacy impacts" (ibid. iv).

PIAs are the immediate precedent for Data Protection Impact Assessments (DPIAs), as foreseen by the EU Directive proposal. The IA Document defines DPIAs as a PIA[35]:

> "A process whereby a conscious and systematic effort is made to assess privacy risks to individuals in the collection, use and disclosure of their personal data. DPIAs help identify privacy risks, foresee problems and bring forward solutions".

Two of the authors which have been consistently working on IAs and Privacy so far, David Wright and Paul de Hert (2012, 7 and ff.), examined recently several definitions of PIAs, finding a considerable similarity in the principal ideas. A PIA is conceived as a *methodology* and *process* for identifying and evaluating risks to privacy, checking for compliance with legislation and aiming at avoiding or mitigating those risks. Thus, three elements should be considered and identified to carry out it: (i) vulnerabilities of assets (defined according to the ISO/IEC 27005:2008 standard: anything that has value to an organisation and which therefore requires protection) , (ii) threats (defined as an aspect of a system or process that can be exploited for purposes other than those originally intended) (iii) and risks (defined according to the ISO/ 27005 standard:2008 as the potential that a given threat will exploit vulnerabilities of an asset or group of assets and cause harm to the organization).

According to the guarantees raised by the rulings of the European Court of Human Rights, Paul de Hert has championed a human rights-based approach to PIAs. Therefore, a "true" PIA departs from the "permissible limitation test" consisting of the seven elements identified by the ECtHR in the context of Art. 8 ECHR (de Hert, 2012, 59 and ff.) :

1. The technology should be used in accordance with and as provided by the law
2. The technology or processing should serve a legitimate aim
3. The technology should not violate the core aspects of the privacy right
4. The technology should be necessary in a democratic society
5. The technology should not have or give unfettered discretion
6. The technology should be appropriate, least intrusive and proportionate

---

10. The Role of the Oversight Agency. Clarke concludes (2010): "The four jurisdictions whose guidance documents the analysis shows to stand out as best practice publications are (in chronological order by original publication date) those of Ontario (1999/2001 and 2005), Alberta (2005/2009), the UK (2007), and Victoria (2009)".

[34] Available at http://privacy.org.nz/privacy-impact-assessment-handbook/

[35] See esp. Annex 6. "The cost of a DPIA inherently involves a case-by-case calculation, depending on the nature and scale of the exercise. However, this obligation would be foreseen only for those data processing presenting specific risks to the rights and freedoms of data subjects. The threshold in the criteria for the applicability of this provision would be narrowly and precisely defined to ensure that its scope would not be disproportionately wide". Op. cit. pp. 69-70.

7. The technology should not only respect privacy requirements but also be consistent with other human rights

De Hert is explicit about the consequences of the democratic political content of his approach:

> Checking on data protection requirements is important but drawing a line between illegitimate and legitimate use of power in a democratic State by answering the question "What kind of processing do we really *not* want?" sometimes comes first. *Innocent people should not be included in databases dedicated to criminal identification and mainly destined to the storage of data of convicted people. The mere storage of such information conveys by itself a risk of stigmatisation; shadows of suspicion are projected upon those whose data is stored. Therefore, the storage of such data, when related to non-convicted individuals, has to be limited and stopped* [emphasis added] (de Hert, 2012, 57-58).

¿Should PIAs be extended to security? ¿Should they be applied to monitor the CAPER platform?

Raab and Wright (2012, 379) elaborate what they call "PIA Circles": protection slides from the inner circle (individual privacy) towards the outer ones. PIA 1 focuses on individual privacy; PIA 2 focuses on the former one and on other impacts on individual's relationships and freedoms; PIA 3 focuses on PIA 2 and on groups and categories; PIA 4 focuses on PIA 3 and impacts on society and the political system (Fig. 2).

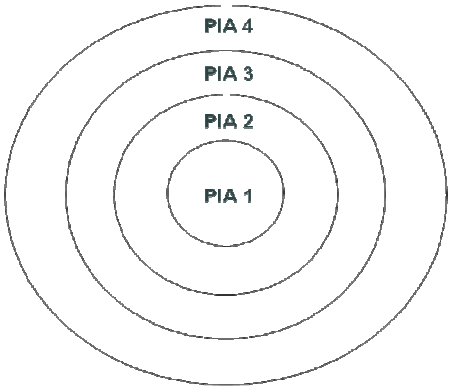

Fig. 2. Extended limits of PIA: Circles of PIA.
Source: Raab and Wright (2012, 379-380)

The aim is expanding protection to other roles and functions of the administration and government under the rule of law. This approach is not new. In a way, CAPER is *a* "dataveillance" platform. *Dataveillance* means "'the systematic monitoring of people's actions or communications through the application of information technology" (Clarke, 1988). The same Roger Clarke explains the origins: "I coined 'dataveillance' in the mid-1980s. The purpose was to draw attention to the substantial shift that was occurring from (expensive) physical and electronic surveillance of individuals to (cheap) surveillance of people's

behaviour through the increasingly intensive data trails that their behaviour was generating."[36]

However, perhaps the difference between a PIA and a DPIA approach lies in the different conception of the state under the rule of law (common law) and the *état de droit, estado de derecho, stato di* diritto*, Rechtsstaat* (civil law). The IA Document for the new EU regulations assumes the benefits of such a projection of privacy to freedom, justice and security:

> The extension of general data protection principles to this area would have a positive impact on the standards of protection, and thus on individuals' data protection rights, in particular by strengthening the rules on right of access, transparency and on purpose limitation.[37]

This is both reflected into the present Draft for the new Directive and Regulations (the Vivian Reding Draft) and into the main suggestions drafted by the European Parliament's rapporteur Jan Philipp Albrecht (Committee for Civil Liberties, Justice and Home Affairs / LIBE) for the new Directive and Regulations reflect these protective trends towards citizens' personal data in Europe. Albrecht's proposal is particularly critical with the invasive actions taken by big companies (Facebook and Google e.g.) and states:[38]

- *Limit exception clauses:* Exceptions from the rules of the regulation should be strictly limited to what is really necessary.
- *Informed consent as a cornerstone*: Users must be informed about what happens with their data, and they must be able to consciously agree to data processing – or reject it. Terms of use must be easy to comprehend, and standardised icons should replace pages and pages of legalistic language in current privacy policies.
- *Technical standards*: Website owners and third parties should not be allowed to track users and create profiles if the privacy settings of the browser signal that the user does not want this. It should be possible to declare such technical data protection standards as legally binding.
- *Privacy by Design / Privacy by Default:* Data processors as well as producers of IT systems should design their offers in a data-minimising way and with the most data protection-friendly pre-settings. A strong principle of purpose limitation means that only data necessary for the provision of a service are processed. It should also be possible to use services anonymously or pseudonymously.
- *Right to data access, correction, and erasure:* Providers should explain in an easily understandable way, free of charge, and quickly which user data they process in which context, and hand over these data electronically on request. For the "right to beforgotten", a meaningful balance between Freedom of Expression and Data Protection must be struck. Furthermore, this right should only be valid if the person concerned had not agreed to the publication of her data.

[36] http://www.rogerclarke.com/DV/
[37] Op. cit p. 110
[38] http://www.janalbrecht.eu/uploads/pics/data_protection_English.pdf (20 December 2012). This is a summary of the Draft Report on the proposal for a regulation of the European Parliament and of the Council on the protection of individual 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)), 17 December 2012.

- *Less red tape:* The internal data protection officer will help companies comply with the law. In return, overly burdensome provisions in the proposed regulation should be deleted. The appointment of a data protection officer should depend on the amount and relevance of data processing, not on the size of a company.
- *Harmonised enforcement of the rules:* Data protection authorities need comparable resources and staff. The European Data Protection Board should be empowered to effectively decide about the EU-wide interpretation of the law. The criteria for the amount of administrative sanctions should be more clearly defined.
- *One counterpart for all of Europe:* For citizens as well as companies, the „one-stopshop"- approach should ensure they only have one data protection authority in the whole EU to deal with. Citizens can go to their data protection authority for complaints that cover data abuse anywhere in the EU. Companies will only have to deal with the authority in the country of their main establishment. The rapporteur proposes a number of improvements on the coordination and decision-making among the national authorities.

Actually this is not going without controversy (Lischka and Stöcker, 2013). The Reding draft does not go that far. Albrecht's proposal is a modified version reflecting the concerns of the European legislative body because the new regulation is in fact more restrictive and less protective than the present one under the 1995 and 2002 Directives. Both drafts are according more regulatory power to the proposed European Data Protection Board, thus limiting the powers of national-states. But the role of security and the interpretation of the exception for security matters in Recital 14 are slighltly different.[39]

3.3.2 Privacy by Design (PbD) and Open Linked Data (OLD)

The "*Data protection by design"* principle has been adopted as well as a general principle. The IA Proposal states:

> New and harmonised provisions which clarify the legal obligations for the processor, irrespective of the obligations laid down in the contract or the legal act with the controller, as well as the application of the "data protection by design" principle, the need for data protection impact assessments in some cases, and an obligation to

[39] Cfr. the original writing and the proposed amendment of Recital 14 of the proposed Regulation: *Text proposed by the Commission: "*(14) This Regulation does not address issues of protection of fundamental rights and freedoms or the free flow of data related to activities which fall outside the scope of Union law, nor does it cover the processing of personal data by the Union institutions, bodies, offices and agencies, which are subject to Regulation (EC) No 45/2001, or the processing of personal data by the Member States when carrying out activities in relation to the common foreign and security policy of the Union". Amendment: "(14) This Regulation does not address issues of protection of fundamental rights and freedoms or the free flow of data related to activities which fall outside the scope of Union law, nor does it cover the processing of personal data by the Union institutions, bodies, offices and agencies, which are subject to Regulation (EC) No 45/2001 *of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data*, or the processing of personal data by the Member States when carrying out activities in relation to the common foreign and security policy of the Union. *In order to ensure a coherent data protection framework, Regulation (EC) No 45/2001 should be brought into line with this Regulation"*.

cooperate with supervisory authorities will bring about benefits for the individual, as this will ensure that outsourcing and delegation by controllers to processors do not result in lowering the standard of data protection.[40]

This is a step ahead to implement privacy by design technologies to regulations. Ugo Pagallo (EC) mentioned PbD in his report and asked for the need to incorporate it as a companion to the CAPER regulatory strategy ("security by design"): "CRM can benefit from the remarks of Ann Cavoukian and Jeff Jonas in *Privacy by Design in the Age of Big Data* (8 June 2012)".

Cavoukian and Jonas (2012) and Jonas (2012a,b,c) are proposing the extension of the Cavoukian seven foundational principles of privacy by design (already described in D7.1, 1.4.1) to Open Linked Data (OLD).

- self-correcting false positives-approach, so that "with every new data point presented, prior assertions are re-evaluated to ensure they are still correct, and if no longer correct, these earlier assumptions can often be repaired – in real time" (see above, 1.2.1)
- That is to say: refining the principle of accountibility, and special attention should be drawn to the criteria of full attribution, data tethering, and tamper-resistant audit logs.

Jonas's sensemake systems would incorporate these PbD features (Cavoukian and Jonas, 2012):

1. *Full attribution*: Every observation (record) needs to know from where it came and when. There cannot be merge/purge data survivorship processing whereby some observations or fields are discarded.

2. *Data tethering*: Adds, changes and deletes occurring in systems of record must be accounted for, in real time, in sub-seconds.

3. *Analytics on anonymized data*: The ability to perform advanced analytics (including some fuzzy matching) over cryptographically altered data means organizations can anonymize more data before information sharing.

4. *Tamper-resistant audit logs*: Every user search should be logged in a tamper-resistant manner — even the database administrator should not be able to alter the evidence contained in this audit log.

5. *False negative favoring methods*: The capability to more strongly favor false negatives is of critical importance in systems that could be used to affect someone's civil liberties.

6. *Self-correcting false positives*: With every new data point presented, prior assertions are re-evaluated to ensure they are still correct, and if no longer correct, these earlier assertions can often be repaired —in real time.

[40] Op. Cit. p. 109

7. *Information transfer accounting*: Every secondary transfer of data, whether to human eyeball or a tertiary system, can be recorded to allow stakeholders (e.g., data custodians or the consumers themselves) to understand how their data is flowing.

As a program, this goes far beyond the CAPER project. But anonymized data, false negatives and self-correcting false positives constitute topics to be tackled in the construction of the CAPER platform. These problems have to be faced.

What it is valuable from the EC first reports is that they situate the CAPER project in this perspective of cloud computing, big data, OLD and second generation of Semantic Web developments. In a way, they observe that through this kind of platforms, crawling will reach all kind of data, and web services providers and controllers cannot ignore the effects produced by the shift from Web 1.0 to Web 2.0 and Web 3.0.

In fact, we can notice that there is a renewal of the interest for ethical principles and regulations in nearly all technological fields as the Web changes. There is a synergy then between the following positions (already referred in D7.1):

- Linked Open Data Principles (T. Berners-Lee, 2006)
- Internet Identity Metasystem Layer: Laws of Identity (Kim Cameron, 2005)
- Privacy by Design Foundational Principles (Ann Cavoukian, 2006)
- The Global Privacy Standard (Cavoukian, 2007)
- Legal Information Institute Standards (Déclaration de Montreal, LAW.GOV Principles, The Hague Principles… 2002-2012)
- Principles on Freedom, Security and Justice settled by Article 29 (Directive 95/46) Data Protection Working Party back in 1997!

Those last Principles are well-known as they were implied, developed and implemented in the Directive Directive 95/46/EC:

- The purpose limitation principle
- The data quality and proportionality principle
- The transparency principle
- The security principle
- The rights of access, rectification and opposition
- Restrictions on onwards transfers

Table 2 and Figure 3 summarize and show a comparison between principles of the different fields, deepening into Cameron (2005) and Cavoukian (2006, 2010) first proposals and expanding them through the Semantic Web area and the Legal Information Institutes principles.

Privacy by Design Foundational Principles	Fair Information Practice Principle (GPS)	Extended Principles	Semantic Web LOD Governemnt	LII Principles
1. Proactive not reactive; Preventative not Remedia		Demonstrable commitment to set and enforce high privacy standards. Evidence that methods to **recognize** poor privacy designs, to **anticipate** poor privacy practices and outcomes, and to correct the negative impacts proactively are established.	Proactive modeling: XML, RDF, SPARQL, OWL	Technological investment
2. Privacy as the Default Setting	3. Purpose Specification 4. Collection Limitation, Data Minimization 5. Use, Retention and Disclosure Limitation	Privacy as the default starting point for designing and operating Information technologies and systems represents the maximum personal privacy that one can have. That is, privacy becomes the prevailing condition -without the data subject ever having to ask for it -no action required.	Access, Data, Storage, Metadata, Ontologies, Alarm Systems, Trust	Republication, Anonymization
3. Privacy Embedded into Design		Systemic program or methodology in place to ensure that privacy is thoroughly integrated into operations. It should be standards-based and amenable to review and validation All privacy threats and risks should be identified and mitigated to the fullest extent possible in a documented action plan.	Architecture, Data protection, Storage, Metadata, Enrichment, Core Ontologies, Domain Ontologies, Rules, Principles, Trust, Validation	Republication Reusing Authentication (Authortative versions) Integrity
4. Full Functionality – Positive-Sum, not Zero-Sum		All legitimate non-privacy interests and objectives are identified early, desired functions articulated, agreed metrics applied, and unnecessary trade-offs rejected in favour of achieving multi-functional solutions.	Access, Data protection, Metadata, Core Ontologies, Domain Ontologies, Rules, Principles, Trust, Validation	Balanced interests (publisher/state/user)
5. End-to-End Security Full Lifecycle Protection	7. Security		Ontology sustainability, folksonomies	Integrity, Security, Maintenance
6. Visibility and Transparency – Keep It Open	2. Accountability 8. Openness 10. Compliance		Accountable information systems and decisions; Content value, tagging and semantic enrichement	Accountability, Distributed Authority of republished materials
7. Respect for User Privacy – Keep it User-Centric	1. Consent 6. Accuracy 9. Access		End user-centered systems, personalization, middle-out ontology approach	Consent , Integrity, Content and added value preservation

Table 3. Comparaison of fundamental regulatory principles across domains (Privacy, LOD, LII). Source: Cameron (2005), Cavoukian (2006, 2010)/ Casanovas (2012).

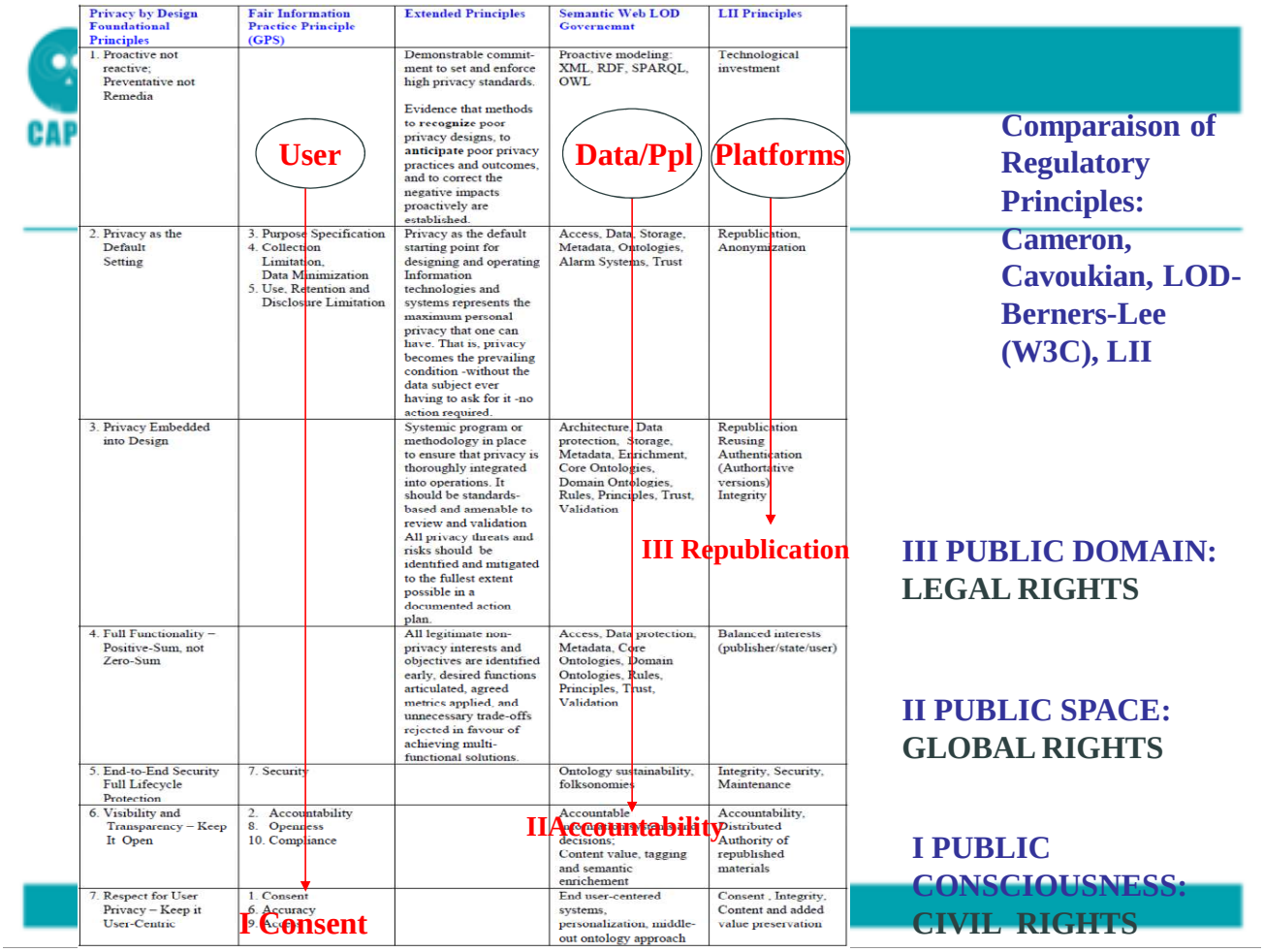

Fig. 3. Redefinition of the public space: legal rights, global rights, civil rights.

Users, data/people (protocols) and platforms (applications) are only the main focus of different approaches to which different regulatory systems can be implemented: law, policies, ethics… Public consciousness, public space, and public domain can be defined from all sides, but with different weight or attention.

- **I Public consciousness**: Civil rights – Ethics, constitutional (national) principles, international courts and law are involved. Criterium: Personal intimacy (e.g. protection of public image) Consent
- **II Public space**: Global Rights – Ethics, constitutional (national) principles, international law and courts are involved. Criterium: Political integration and development (e.g. accessibility to information) Accountability
- **III Public domain**: Legal Rights – Ethics, constitutional (national) principles, international property law and courts are involved. Criterium: Public / Private domain (eg. intellectual property: protection of the created added value) Republication

In this broad redefinition of the public space, national security has a place, and certainly an important one, but it has to be re-shaped in the light of the wide open possibilities of the new Directive and Regulations. This is what we tried to incorporate into the CRM.

3.3.3 Next steps for CRM

What are the most fruitful regulatory steps to be followed in the justice, security and freedom area to reach an agreement, and thus, to be effectively implemented in CAPER?

The high complexity and transitory stage of Privacy and Data Protection regulations in Europe is a call for prudence to build the CAPER Regulatory Model.

The CRM is not an ethical code, and only in the broadest sense can be taken for a PIA. It is not a cost-benefit analysis, it is not aiming at evaluating a public policy or a technical tool, but at bringing together all the relevant values, principles, policies and concrete regulations to anticipate and eventually solve conflicts among partners, LEAs and citizens. It has some features in common with codes (an ordered body of guidelines), with best practices (a recommended set of behaviors) and PIAs (a risk analysis to prevent future pitfalls of the system). In this sense, CRM operates as a knowledge ruler.

The final output would be (i) a set of specific recommendations separately laid down for LEAs and partners; (ii) a set of specific rules to be taken into account and implemented into the CAPER technical building; (iii) a set of specific values and principles to be evaluated by the CAPER Ethical Committee; (iv) a theoretical model, that sets apart the networked and multi-levelled regulation which is needed in technological and organizational management.

A first set of recommendations will serve as a template for the ethical audit. In the next sections we will describe first the state of the relevant legal materials, before introducing the first recommendations presented before the Ethical Committee. To make them up, we took into account not only the present valid law (the way in which legislation and Directives are applied and interpreted in court), but the state of the art of legal doctrine and the most relevant court rulings.[41] Special attention has been paid to best practices guides for technology and research.[42]

[41] For LEAs, *inter alia*: *European Court of Human Right (ECtHR), S. and Marper v. the United Kingdom*, Application nos. 30562/04 and 30566/04, judgment of 4 December 2008; *ECtHR, Weber and Saravia v. Germany*, Application no. 54934/00, admissibility decision of 29 June 2006; ECtHR, *Kennedy v. the United Kingdom*, Application no. 26839/05, judgment of 18 May 2010 and *Kvasnica v. Slovakia*, Application no. 72094/01 of 9 June 2006; *ECtHR, Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria,* Application no. 62540/00, judgment of 28 June 2007; *C.G. and others v. Bulgaria*, Application no. 1365/07, judgment of 24 April 2008. *ECtHR, Segerstedt – Wiberg and others v. Sweden*, Application no. 62332/00, judgment of 6 June 2006; *Knauth v. Germany*, Application no. 41111/98, admissibility decision of 22 November 2001; ECtHR, Cases T-228/02, *Organisation des Modjahedines du people d'Iran v. Council*, judgment of 12 December 2006; T-284, *Organisation des Modjahedines du peuple d'Iran v. Council*, judgment of 4 December 2008; Case T-47/03, *Sison v. Council,* judgment of 11 July 2007; C-266/05 P, *Sison v. Council*, judgment of 1 February 2007 and C-229/05 P, *PKK and KKK v. Council*, judgment of 18 January 2007;ECTHR, C-524/06 *Heinz Huber v.*Germany, judgment of 16 December

2008. European Data Protection Supervisor, *EURODAC Central UNIT; Inspection Report. June 2012, Case file: 2011-2013;* European Data Protection Supervisor, *Security Audit VIS Central System. Summary Report. 1 June 2012.*Public 38/66; European Network and Information Security Agency (ENISA), *Privacy, Accountability and Trust – Challenges and Opportunities*, Feb 2011.

[42] For reasearchers: Opinion 02/2010 of art. 29 Data Protection Directive Working Group on online behavioural advertising, adopted on 22 June 2010 and Opinion 16/2011 on EASA/IAB Best Practice Recommendation on Online Behavioural Advertising; Opinion 2/2012 of the Article 29 Data Protection Working Group (FACIAL RECOGNITION); Opinion 1/2008 on data protection issues related to search engines adopted on 4 April 2008; UK Data Archive, *Managing and sharing data*. *Best Practice for Researchers*, University of Essex, March 2011. Saint Mary's University Data Storage Guidelines, November 2007; The Australian Code for the responsible Conduct of Research, available at http://www.nhmrc.gov.au/index.htm .

4 DATA PROTECTION GENERAL FRAMEWORK ON ORGANISED CRIME AND TERRORISM: A PATCHWORK

4.1 Public international instruments of the Council of Europe (Convention nº 108, Recommendation R(87) and the European Court of Human Rights (ECtHR) standard)

4.1.1 ECHR Data Protection standard

Before the enactment of the Framework Decision 2008/977/JHA, the Data Protection standard for terrorism and organised crime was based on public international instruments and guarantees. The decisions of the ECHR related to the former EU Third Pillar (Judicial and Police cooperation) and Second Pillar (National security) are more relevant than those of the EU Justice Court to our purpose, for EU Courts had limited competences in the former third pillar. Yet, this might change now after the Lisbon Treaty. Let's start now with the ECHR decisions.

a) Retention of Information Related to Criminal Offences Including Biometric

In a 2008 Decision[43], the ECtHR developed an important general framework on minimum data protection standard in databases serving crime detection and prevention. The following rules are to be considered (Bohem, 2012, 62):

- The presumption of innocence demands a different treatment of data of people who have been convicted of an offence and those who have never been.
- A distinction has to be made between serious and less serious offences.
- The age of the suspected has to be taken into account.
- Possibilities to have the data removed from the database have to be established.
- Provisions for independent review of the justification for the retention according to defined criteria, such as the seriousness of the offence, previous arrests, the strength of the suspicion against the person and any other special circumstances, have to assure the lawfulness of the provided measure.
- Retention has to be limited in time.

b) Data collection, Storing and Retention with Regard to Measures Against Terrorism and Transmission of Data to Third Parties

In a 2006 Decision[44], the ECtHR summarizes the principles that national states must respect when enacting legislation on combating terrorism and other serious crimes. The essential

[43] *S. and Marper v. the United Kingdom*, Application nos. 30562/04 and 30566/04, judgment of 4 December 2008.

requirements in compliance with Article 8 of the European Convention on Human Rights (ECHR) are (Bohem, 2012, 67):

- Limitation on the categories of individuals against whom surveillance measures may be taken
- Determine which kind of data are to be stored and for which purposes the data will be used afterwards
- Clear definition of the limits of the storing and the use of information before processing
- Time limits for storing
- Avoid indiscriminate storing of data, for instance taking into account the age of the person concerned
- Independent control of the surveillance of measures and of the data obtained through it.
- Retention has to be proportionate in relation to the purpose of collection and limited in time
- Adequate procedures for preserving the data's integrity and confidentiality
- Procedures for the destruction of the data
- Remedies in case of misuse
- Information of the people concerned after the termination of the measures.
- Limited types of offenses behalf of which data transmission is permitted.
- Data transmitted must be marked and remain connected to the purposes which had justified their collection
- The transmission must be collected in minutes

c) Surveillance measures

The ECtHR has accepted that national authorities enjoy a fairly wide margin of appreciation in selecting the means for achieving the aim of protecting national security (Bohem, 2012, 70). However, in two 2007 and 2008 Cases[45], the ECtHR establishes the essential guarantees and requirements for surveillance legislation:

- Independent control during and after the exercise of secret surveillance measures
- Information of the person concerned after the termination of the measures

The ECtHR insists that basic data protection principles also apply within the framework of secret surveillance measures.

d) Secret Security Files

In two 2001 and 2006 Decisions[46], the ECtHR is confronted with the question of whether the continued storage of secret service information is justified. The rule is (Bohem, 2012, 74-75):

[44] *Weber and Saravia v. Germany*, Application no. 54934/00, admissibility decision of 29 June 2006. The standards are confirmed by cases *Kennedy v. the United Kingdom*, Application no. 26839/05, judgment of 18 May 2010 and *Kvasnica v. Slovakia*, Application no. 72094/01 of 9 June 2006.
[45] *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria,* Application no. 62540/00, judgment of 28 June 2007; *C.G. and others v. Bulgaria*, Application no. 1365/07, judgment of 24 April 2008.
[46] *Segerstedt – Wiberg and others v. Sweden*, Application no. 62332/00, judgment of 6 June 2006; *Knauth v. Germany*, Application no. 41111/98, admissibility decision of 22 November 2001.

- Indefinite storage is exceptional and needs justification for the protection of national security
- Retention of rather old (30 years) and fairly harmless data is not necessary any longer
- There is a right to erase information which is no longer relevant for the protection of national security or the prevention of disorder and crime
- The use of data obtained by a former secret service is to be used only if the state pursued a legitimate aim and the measure at issue is essentially necessary in a democratic society

e) Access to Secret Service Files

In an above mentioned 2008 Case[47], the ECtHR clarified that (Bohem, 2012, 79):

- States are not under a general obligation regarding a right of full access to secret service data files
- Nevertheless there is a right to know whether the content of one's secret service data file was lawfully created if restrictive measures against a person concerned are based on this secret information
- The right of access to a secret file can be included in Article 6 ECHR as part of the right to a fair trial

f) Rectification and Erasure

In the two above mentioned Cases of 2006 and 2008[48], the ECtHR becomes increasingly aware of the rectification and erasure rights:

- Right to erase data if they are wrong or no longer needed to safeguard an "actual relevant national security interest"
- The participation in a political meeting or the entry about resistance to police control during demonstrations 30 years ago are examples of information no longer relevant to national security

3.1.2 Data protection standards in the Council of Europe Convention no. 108[49]

[47] *C.G. and others v. Bulgaria*, Application judgment of 24 April 2004.
[48] *Segerstedt – Wiberg and others v. Sweden*, Application no. 62332/00, judgment of 6 June 2006; *S. and Marper v. the United Kingdom*, Application nos. 30562/04 and 30566/04, judgment of 4 December 2008.
[49] Council of Europe Convention no. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data, 28 January 1978.

Five basic data protection standards refer to quality of data and data processing. Data must be:

- Obtained and processed fairly and lawfully
- Stored for specific and legitimate purposes and not used in a way incompatible with those purposes
- Adequate, relevant and not excessive in relation to the purposes for which they are stored
- Accurate and, where necessary, kept up to date
- Preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored

Derogation of this five principles must be provided by national law and must constitute a "necessary measure in a democratic society in the interest of: protection state security, public safety, the monetary interest of the state or the suppression of criminal offences" or the protection of the data subject's rights of others.

Some additional provisions are required:

- Establish provisions regarding "special categories" of data[50]
- Sanction and remedy system for people concerned

An Additional Protocol Amending Convention no. 108 regarding supervisory authorities and transborder data flows was enacted in 2001[51].

3.1.3 Recommendation No. R(87) 15 Regulating the Use of Personal Data in the Police Sector

This Recommendation entails important and basic data protection principles for the police sector. The most relevant points for the CAPER project are (Bohem, 2012, 102):

- Comprehensive independent control and supervision established outside the police sector (principle one). A number of EU instruments refer to this Recommendation and scholars held that the same principles should also apply to supervisory authorities at the EU level.

- Strict limitation of the collection of data to police purposes for reasons such as the prevention of a real danger or the suppression of specific criminal offences. This is more restrictive than the current broader scope of today's mechanisms of data exchange, notably the Data Retention Directive, The Europol-US agreement on data and related information exchange and the PNR agreement between the US and the

[50] The notion of "special category" has an anti-discriminatory function and refers to data revealing racial or ethnic origin, political opinions, religious or other beliefs, health or sexual life or criminal convictions. Nowadays the term "sensitive data" is more usual for these data.
[51] Additional Protocol of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows, 8 November 2001.

EU. On the contrary, the Recommendation's principle excludes the open-ended and indiscriminate collection of data by the police.

- The data transferred to other public bodies, private parties and foreign authorities should not be used for purposes other than those specified in the request for communication. This provision applies to all EU's police data exchange data systems referring to Recommendation R (87) 15. Problems arise when third states do not always agree to a limited use of data once obtained, or when the purpose is not concrete and there is no specification of the precise use of the data.

4.2 A missed opportunity to create a legal data protection framework (Framework Decision 2008/977/JHA)

Data processing in the third pillar matters was exclusively governed up to 2008 by public international law instruments of the Council of Europe (Convention 108, Recommendation R (87) 15 and the ECtHR standard).

The Data Protection Framework Decision 2008/977/JHA on personal data processed in the framework of police and judicial cooperation was finally adopted in November 2008[52]. A great opportunity to create a data protection framework in the former third pillar was missed due to several factors:

- Restricted scope of the Framework Decision, neither applicable to the data processing of most of the AFSJ law enforcement agencies, such as Europol and Eurojust, nor to other AFSJ exchange systems like SIS or CIS. The internal processing of the Member States in police and criminal matters is also excluded.

- Exclusively application in a cross-border context, and even there with exceptions, like the cross-border DNA information exchange between Member States, ruled by the Treaty of Prüm[53].

- Low level of protection.

- Lack of specific rules in police and criminal cooperation.

The entry into force of the Treaty of Lisbon (TFEU) influenced the Framework Decision in several ways:

- It abolished the EU three pillar structure introduced with the Treaty of Maastricht on 1 November 1993.

[52] Council 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, OJ L 350, 30.12.2008, p. 60 ('Framework Decision'). Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:350:0060:01:EN:HTML

[53] The Treaty of Prüm was signed in May 2005 and contains provisions about cross-border cooperation, particularly in combating terrorism and cross-border crime. Council Decision 2008/615/JHA, of 23 June has transposed it in EU Law.

- Introduced in Article 16 TFEU the subjective right to data protection applicable to all data processing in public and private matters, including the AFSJ.

- It reserved the possibility to enact in national security and in police and judicial cooperation other general data protection rules applicable to the former first pillar (Declarations 20 and 21 annexed to the TFEU).

- Protocol No. 21 annexed to Treaty of Lisbon provides also for derogations for the U.K. and Ireland. Protocol No. 22 does the same for Denmark.

- Protocol No. 36 stipulates a delay in the application of the guarantees set out by Article 16. The transitional provisions allowed that rules and instruments adopted prior to the Lisbon Treaty would remain untouched as long as they were not modified, repealed or annulled.

As a result, an enormous legislative activity took place right before the entry into force of The Lisbon Treaty. Many instruments in the AFSJ like Europol and Eurojust Decisions and their implementing measures or the law enforcement access to VIS do not comply with the data protection guarantees of Article 16 of the Lisbon Treaty (TFEU) in the AFSJ. Yet, they remain applicable to domestic data processing in police and judicial matters (Bohem, 2012, 119-20).

- The establishment of the permanent standing committee, COSI (Comité de Sécurité Intérieure) in Article 71 TFEU coordinating the internal security policy.

The Council Framework Decision has weak data protection quality standards compared to the Data Protection Directive:

- **Purpose limitation principle**[54]
  Only competent authorities may collect personal data under specified, explicit and legitimate purposes. Principles of lawfulness, proportionality and purpose should determine actions regarding data processing by these authorities.

  The purpose limitation framework allows thus the authorities processing the data to decide about the change of the purpose. Doing so, the initial aim of this principle, the protection of individuals against the indiscriminate use of personal data, is not completely accomplished.

[54] For the purposes of this Framework Decision the following concepts are defined as: (1) “processing of personal data mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such a collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction”; (2) “competent authorities are agencies or bodies established by legal acts…as well as police, customs, judicial and other competent authorities of the Member States that are authorized by national law to process personal data within the scope of this Framework Decision”; (3) “personal data mean any information relating to an identified or identifiable natural person (‘data subject’); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity”.

Further processing for another purpose is permitted so far as long as[55]:

- It is not incompatible with the purposes for which the data were collected
- The competent authorities are authorized to process such data for such other purpose in accordance with the applicable legal provisions
- Processing is necessary and proportionate to that other purpose

Some reasons for further processing, always complying with the aforementioned principles are:

- Prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties other than those for which they were transmitted or made available
- Prevention of an immediate and serious threat to public security
- Any other purpose only with the prior consent of the transmitting Member State or with the consent of the data subject, given in accordance with national Law.

- **Data must be accurate and where necessary, kept up to date**

Although relevant to police work, the Council Framework Decision does not have any provision on accuracy of data. It makes no distinction on data collected for administrative purposes and data collected for police objectives, or between data based on facts and data based on opinions or personal assessments. The European Data Protection Supervisor has warned that the difference between evidences, facts and opinions or assessments (soft intelligence) disappears when transferring such data to another authority[56].

No distinction is further made between the different categories of data subjects such as criminals, suspects, victims or witnesses (Boehm, 2012, 135).

- **Time limits**

The Framework Decision provides that “personal data shall be erased or made anonymous when they are no longer required for the purposes for which they were lawfully collected or are lawfully further processed”[57].
If at the time of expiration the data are needed for “a current investigation, prosecution of criminal offences or the enforcement of criminal penalties”, this obligation shall not apply[58].

The use of “shall” instead of “must” (Directive and Regulation 45/2001) indicates a slightly mitigated obligation to erase the data or to make them anonymous (Bohem, 2012, 136). If the purpose changes during the processing, the limit can easily be adapted to the new purpose. The close relationship between purpose

[55] Article 3(2) Council Framework Decision.
[56] European Data Protection Supervisor Opinion on the Council Framework Decision, OJ 2007, C.139/1, paragraph 32.
[57] Article 4(2) Council Framework Decision.
[58] Article 9(1) Council Framework Decision.

and the duration of the storage makes it possible that, in practice, the time limit can be indefinitely extended (Bohem, ibid.).

- **Special categories of data**

In contrast to Directive 95/46 and Regulation 45/2001, the Decision Framework does not have a list with a general prohibition of the processing of sensitive data. Article 6 of the Framework Decision allows the processing of data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership and personal data concerning health or sex life when the processing is "strictly necessary and when the national law provides adequate safeguards".

However, even being an instrument for police and judicial cooperation, the Framework Decision does not refer to data related to criminal offences, convictions or security measures, or the biometric data as special categories of data.

- **Rights of Data subjects**

In contrast with 95/46 Directive and 45/2001 Regulation, the Framework Decision does not stipulate a clear obligation to inform the person concerned about the processing. The wording of the Framework Decision appears to be more a possibility than an obligation (Bohem, 2012, 140).

Recital (26) of the framework mentions that "[…] it may be necessary to inform data subjects regarding the processing of their data". In Article 16 we have more details: "Member States shall ensure that the data subject is informed regarding the collection of personal data by their competent authorities, in accordance with national Law".

The right to access in the Framework Decision is limited to[59]:

- Confirmation from the controller or from the national supervisory authority as to whether or not data related to him have been transmitted or made available.
- Information on the recipients or categories of recipients of the information disclosed.
- Confirmation from the national supervisory authority that all necessary verifications have taken place.

As a result, information relating to the purpose of processing, the source or the communication in an intelligible forma are not provided (Bohem, 2012, 142).

In addition to the limited information, various exceptions apply to restrict the access right[60]:

- to avoid obstructing official or legal inquiries, investigations or procedures
- to avoid prejudicing the prevention, detection, investigation and prosecution of criminal offences or for the execution of criminal penalties
- to protect public security

[59] Article 17(1) and Article 17(2) Council Framework Decision.
[60] Article 17(2) Council Framework Decision.

- to protect the data subject or the rights of others

When restricting the access, the measure must be necessary and proportional and Member States must take into account the legitimate interests of the person concerned. In all those case the person concerned "shall be advised that he may appeal to the competent national supervisory authority, a judicial authority or to a court".

The Framework Decision stipulates further guarantees in case the controller refuses rectification, erasure of blocking. Each "refusal must be communicated in writing to the data subject who must be informed of the possibilities provided for in national law for lodging a complaint or seeking judicial remedy"[61].

In case that incorrect data have been transmitted, or data have been unlawfully transmitted, the recipient of the data "must be notified without delay"[62]. The individual is however not notified.

The Framework Decision does not involve a right to object. Scholars held the need for a right to object in police context in situations in which a victim or witness may have legitimate grounds to it (Bohem, 2012, 144).

Instead of the general approach of Directive 95/46 and Regulation 45/2001 to prohibit automated decisions, the Framework Decision generally permits them if they are authorised by law.

- **Data transfer**

The Framework Decision does not regulate the EU-internal data transfer in the framework of police and judicial cooperation.

Recital (23) of the Framework Decision stipulates that when personal data are transferred from a Member State to third states or international bodies, these data should *in principle* benefit from an adequate level of protection[63].

Article 13 of the Framework Decision specifies that personal data may be transferred only if:

- It is necessary for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties
- The receiving authority in the third state or international body is responsible for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties
- The Member State from which the data were obtained has given its consent to the transfer in compliance with its national law
- the third state or international body ensures an adequate level of protection for the intended data processing

[61] Article 18(1) Council Framework Decision.
[62] Article 8(2) Council Framework Decision.
[63] Recital (23) Council Framework Decision, OJ 2008, L-350/60.

Member States may assess the level of adequacy on their own. Very vague and far reaching derogations such as public interests apply. Moreover if a Member State or the EU has already concluded at the time of the adoption of the Framework Decision a bilateral or multilateral agreement with other rules, the latter will apply.

Personal data collected for police and judicial purposes can be transferred to private parties if:

- The competent authority of the country from which the data were obtained has consented to transmission in compliance with his national Law.
- No legitimate specific interests of the data subject prevent transmission
- It is essential for the transmitting authority to[64]:
  . The performance of a task lawfully assigned to it
  . The prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties
  . The prevention of an immediate and serious threat to public security
  . The prevention of serious harm to the rights of individuals

The party transmitting the data shall inform the private party of the purposes for which the data may exclusively be used.

The Framework Decision does not provide any indication on the access of LEAs to data stored in private databases.

- **Security**

Competent authorities must take the necessary security and confidentiality measures of processing (against destruction, accidental loss, alteration and unauthorised access or disclosure) and especially with regard to automated processing of data.

Article 22 of the Framework Decision stipulate 11 measures which shall be implemented to protect personal data in automated data processing systems:

- Equipment access control
- Control of data media
- Storage
- Users
- Data access
- Communication
- Input
- Transport
- Recovery
- Reliability
- Integrity

[64] Article 14(1) Council Framework Decision.

4.3 EU Data Protection General Legal Framework on police and judicial cooperation

The centerpiece of existing EU legislation on personal data protection is the Directive 95/46/EC[65]. Other instruments that include data protection provisions relevant in the AFSJ are Regulation 45/2001 and the Framework Decision before mentioned. The principal aims of the Directive were: (1) to protect the fundamental right to data protection and; (2) to guarantee the free flow of personal data between Member States.

The scope of Directive 95/46 is limited and does not refer to security-related data processing in the AFSJ. Its principles are nonetheless applicable to instruments like VIS or Eurodac, and the supervision of the European Data protection Supervisor adds further guarantees[66].

a) Lawfulness and Fairness

The European Court of Justice put emphasis on the discriminatory effect on a specific group of people whose data are stored in a database use for crime fighting purposes. The judgment additionally takes into account that the purpose of processing of the data is changing: data are originally collected for statistical purposes and later used for other purposes.

In the case *Huber v. Germany* the EU Court establishes a data protection regime for police investigations[67]. Mr Huber, an Austrian national lives in Germany where he develops his professional career considers that he was being discriminated against on account of the entry of his personal data into a German centralised register. His personal data (basic data and other type of data regarding any information concerning details of expulsion proceedings, involvements in terrorist activities or serious crimes…) was processed by a centralised register which contains information relating to foreign nationals (EU citizens and non-EU citizens). These data could be processed by different purposes: statistical, to apply legislation concerning the right of residence, and for the purposes of fighting crime.

Two principal legal arguments were pointed out by the Court in this case: (1) with regard to data processing for statistical purposes, the Court considered that statistics on population movements within a concrete territory do not necessitate the collection and storage of individualised information. In addition, the requirement of necessity within the meaning of Directive 95/46/EC was not satisfied; (2) in relation to the fight against crime, the Court stressed that the objective within this area is the prosecution of crimes and offences committed, irrespective of the nationality of their perpetrators. In this case, the German register does not contain personal data of German nationals, and the situation of the nationals of a Member State (MS) cannot be different from the nationals of other MS. In that sense, the court determined that "the systematic processing of personal data only to

[65] Directive 95/46/EC of the European Parliament and of 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, OJ L 281, 23.11.1995, p.31. Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

[66] Supervision of SIS II is intended in future.

[67] C-524/06 *Heinz Huber v.*Germany, judgment of 16 December 2008.

nationals of other MS for the purposes of fighting crime constitutes discrimination on grounds of nationality which is prohibited by Article 12 EC".

A database used for crime investigation can be discriminatory if it contains only the data of a particular group of people. The Court concludes that data protection principles also apply, in some way, in the former third pillar (police and judicial cooperation).

b) Purpose limitation

Directive 95/46 does not specify which purposes are incompatible with the original purpose. Regulation 45/2001 allows changing the original purpose if" the change of purpose is expressly permitted by the internal rules of the Community institution or body"[68].

c) Time limit

According to Directive 95/46 and Regulation 45/2001, data "must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed"[69].

d) Transfer of personal data

The rules of Regulation 45/2001 (for data processing of the institutions and bodies of the European Union) are not applicable to the data processing of former third pillar actors or databases, such as Europol, Eurojust or CIS. Regulation 45/2001 ensures the application of Directive 95/46 to former first pillar EU institutions and bodies.

e) Data Protection General Legal Framework on Common Foreign and Security Policy (terrorism)

With regard to terrorism, there is no harmonised standard or general framework governing data processing. Some elements of data protection to guarantee the protection of other fundamental rights are present in these cases. For instance, the right to defence and judicial protection are mentioned by the Court. Although no right to access personal data is recognised, a right to be informed about the nature and cause of the accusations against someone and a right to access documents held by the Council is progressively been held (Bohem, 2012, 179).

EU Courts have established case law on the management of the so called terrorists' blacklists[70]:

[68] Article 6(1), Regulation 45/2001.
[69] Article 6(1) Directive 95/46 and Article 4(1) (e) Regulation 45/2001.
[70] Cases T-228/02, *Organisation des Modjahedines du people d'Iran v. Council*, judgment of 12 December 2006 ; T-284, *Organisation des Modjahedines du peuple d'Iran v. Council*, judgment of 4 December 2008 ; Case T-47/03, *Sison v. Council,* judgment of 11 July 2007; C-266/05 P, *Sison v.*

"[…] the parties concerned will be informed that the Council intends to maintain them on the list and will be informed via a <<statement of reasons>> of the specific information that forms the basis for the Council's decision"[71].
"The people, groups and entities concerned will also be informed about the opportunity to make their views known and present observations"[72].
The Council will also "consider any reaction by the parties concerned before taking a final decision"[73].
Member States are thus required to provide information concerning the reasons of the placement of certain people on a blacklist[74].

None of the cases directly mention data protection guarantees. Nonetheless, the case-law shows that even in foreign and security policy, terrorism investigation in the context of the CAPER Project, certain data protection elements apply.

With the entry in force of the Lisbon Treaty, the situation for individuals in the area of foreign and security policy has changed and improved. Even the Court of Justice that has in general no jurisdiction with respect to common foreign and security policy cases, has been empowered by Article 275 TFEU in proceedings "reviewing the legality of decisions providing for restrictive measures against natural or legal persons adopted by the Council on the basis of Chapter 2 of Title V [specific provisions on common foreign and security policy] of the Treaty on European Union".

4.4 Concrete Data Protection rules for databases and systems of information exchange between Law Enforcement Agencies within the EU

4.4.1 Schengen Information System II[75]

The second generation Schengen Infomation system (SIS II) is conceived as a general investigative tool. It allows to combine freedom of movement and security within the EU and improve the exchange of information between Member States. Information contained in SIS II is used for control of persons, the issue of visas and resident permits, and for police and judicial cooperation criminal matters.

The legal basis of SIS II are:

Council, judgment of 1 February 2007 and C-229/05 P, *PKK and KKK v. Council*, judgment of 18 January 2007.
[71] Council press release 8425/07 (Presse 80), p.35.
[72] *Ibid*.
[73] *Ibid*.
[74] Boheme (2012, 170)
[75] In 1995 SIS database was created to connect eight countries on the legal basis of the Convention Implementing the Schengen Agreement of 14 June 1985 (OJ 2000 L 239), amended by Council Regulation (EC) 871/2004 of 29 April 2004 concerning the introduction of some new functions for the Schengen Information System, including in the fight against terrorism (OJ 2004 L 162) and Council Decision 2005/211/JHA (OJ 2005 L 68). As it was insufficient, in 1996 the Schengen Committee created a second generation SIS.

Regulation (EC) 1987/2006 of the European Parliament and of the Council (OJ 2006 L 381) of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II)[76].

Council Decision 2007/533 JHA (OJ 2007 L 205) of 12 June 2007 on the establisment, operation and use of the second generation Schengen Information System (SIS II)[77].

Regulation (EC) 1986/2006 of the European Parliament and of the Council (OJ 2006 L 381) of 20 December 2006 regarding access to the Second Generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates[78]

4.4.2 Eurodac

Council Regulation (EC) No 2725/2000 of 11 December 2000 concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention[79]

Eurodac was created in 2003 and it is the first common Automated Fingerprint Identification System (AFIS) within the EU. Eurodac consists of a central unit which includes a database which stores the fingerprints of the following categories of persons: (1) applicants for aylum; (2) aliens apprehended who unlawfully crossed the external borders: (3) and, aliens found illegally present in a Member State.

- **Conditions for access to Eurodac:** no direct access is possible. Requests must be in a hit/not hit process.

4.4.3 Visa Information System (VIS)

COUNCIL DECISION 2008/633/JHA of 23 June 2008 concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences[80]

The Decision states the conditions under which Member States' designated authorities and European Police Office (Europol) may obtain access for consultation of the VIS Information System (VIS) for prevention, detection and investigation purposes related to terrorism offences and other serious criminal offences.

[76] Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:381:0004:0023:EN:PDF
[77] Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2007:205:0063:0084:EN:PDF
[78] Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:381:0001:0003:EN:PDF
[79] Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000R2725:EN:HTML
[80] Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:218:0129:0136:EN:PDF#zoom=100

- Conditions for access to VIS data: The conditions under which designated authorities of the Member States may access to VIS data are the following: (1) when accessing must be necessary; (2) always in a specific case; (3) and, when these authorities have reasonable grounds to consider that consultation of VIS data will contribute in a hard manner to prevent, detect or investigate.
VIS data available for consultation is limited to an specific type of data such as: surname; country, place and date of birth; sex; current nationality and nationality of birth; type and number of the travel document, the authority which issued it and the date of issue and of expiry; main destination and duration of the intended stay; purpose of travel; intended date of arrival and departure; intended border of first entry or transit route; residence; fingerprints; type of visa and the number of the visa sticker; details of the person issuing an invitation and/or liable to pay the applicant's subsistence costs during the stay, photographs (in some cases) and other information made available in VIS System files (also in some cases).

Europol's conditions to access VIS data are fixed by this Decision, and in this respect the main requirement imposed are: (1) when is necessary for developing its tasks, following Article 3 (1), point 2 and Article 10 of the Europol Convention[81]; (2) Europol shall designate a specialised unit for the purpose of this Decision; (3) and, processing of information obtained from VIS shall be restrained to the consent of the Member State which has entered this data in the VIS.

- Protection of personal data: (1) each Member State shall ensure and adequate data protection level in its national law; (2) processing of personal data must be done by Europol in accordance with the Europol Convention and supervised by an independent joint supervisory body; (3) the principle of purpose limitations is applied on protection of personal data; (4) personal data obtained from VIS shall not be transferred or made available to a third country. An exception regarding particular cases of urgency allows the possibility to transfer and make available such data to third countries; (5) in accordance with national law, Member States shall ensure that records are kept of transfers and make them available to national data proteccion; (6) data security measures must be taken to preserve VIS data; (7) each Member State and Eurol shall ensure that all data processing operations linked to acces to the VIS system are recorded with the aim to checking, monitoring, ensuring the optimal functioning of the system, data integrity and security.

Individuals have the right of access, correction and deletion regarding personal data contained in VIS data files.

4.5 Conclusions[82]

1.- All legal instruments presented above have in **common** the following **requirements**:

[81] Europol Convention is available at: http://www.aedh.eu/plugins/fckeditor/userfiles/file/Protection%20des%20donn%C3%A9es%20personnelles/Europol_Convention_Consolidated_version.pdf

[82] These conclusions coincide with the main content of the Communication from the Commission to the European Parliament and the Council. Overview of information management in the area of freedom, security and justice. COM (2010) 385. Available at: http://ec.europa.eu/home-affairs/news/intro/docs/com_2010_385_en.pdf

- All of them are ruled by the principle of limited purpose
- Some of them could present potential overlaps in functioning
- They are limited by controlled access rights
- They are ruled to variable data retention rules
- All of them present effective identity management and data security measures
- All of them recognize rights of individuals to access, correction and deletion of personal data.

2.- **From a policy development perspective**, a set of principles should be taken into account by EU policy makers when presenting proposals involving information management in the area of freedom, security, and justice:

- **Safeguarding fundamental rights**, especially the right to privacy and data protection. This right is a fundamental right included in several legal instruments, as for instance, in article 7 and 8 of the Charter of Fundamental Rights of the EU, or in article 16 of the Treaty on the Functioning of the EU (TFEU). EU policy makers should: (1) consider embedding personal data protection in the technological basis of a legal instrument; (2) establish limitations to data processing in terms of necessity and considering the purpose argued by authorized entities to process personal data; (3) grant data access to authorized entities that really needs to know personal data. That means in practical terms to follow the approach of "privacy by design".

- **Necessity:** Public authorities only must barge in individual's right to privacy in cases of national security, public safety or prevention of crime. When it occurs, the public authorities' action must be submitted to control by an independent authority at national or EU level.

- **Subsidiary and proportionality** must be the interference of public authorities in those cases in which individual's right to privacy is being affected.

- **Accurate risk management** on the basis of real risk, no hypothetical risk. Public authorities should develop risk profiles with the objective of focusing resources on specific individuals when they detect security threats or to protect civil society.

- **Cost-effectiveness:** EU policy makers must consider the option to better use of existing information systems instead of proposing new systems. Mechanism based in adding implemented solutions to existing systems could be a reasonable way to explore.

- **Bottom-up policy design strategy[83]:** any information system in the area of freedom, security and justice must be developed before the underlying legal instruments setting out its purpose, scope, functions and technology details have been adopted. Particular attention must be paid by EU policy makers to the initial design of governance structures.

- **Review and sunset clauses:** proposals in the area of freedom, security and justice will include obligations regarding annual reporting, and periodic and ad hoc review.

[83] See General Principles and Minimum Standards of Public Consultation which are contained in COM (2002) 704, 11.12.2002

5 RISK SCENARIOS OF CAPER USE FOR LAW ENFORCEMENT AGENCIES

Our aim is to adopt a Data Protection Impact Assessment (DPIA) that could be useful to a future legal and ethical framework for the CAPER tool. We will start by defining “risk scenarios”, i.e. the concrete situations in which LEAs will most likely use the tool. We have therefore divided the activities into four successive stages: profiling, storage, management and transfer to third parties.

5.1 Profiling: CAPER data collection

Individuals are now considered as part of a network. The individuality is already present, but delimited in a context. And the context is now linked to the characteristics of the individual. The person is depicted in 3D, with context information that shows his/her daily behaviour.

As a result, the CAPER tool will be used as pre-predictive software for behavioural analyses. The collection of data allows the future analysis for prediction or investigation. The police and terrorist investigation justifies the use of profiling. Nonetheless, some guarantees should be implemented for the collection of data.

- Restriction to open sources: the concept of open source should be clear as a general description: information available with public access. A private profile in a social network is not open source. If someone can access only with the requirement of adopting a password, it is still open source.

- The information collected should also be proportional: the minimum strictly necessary to the investigation. For instance, in the PNR agreement data collected include personal data of people who have decided not to flight in the last 96 hours. This is not proportional and should not be collected.

- No irrelevant personal information should be collected. The challenge here is how to determine relevancy at the very first stages of the collection. Proportionality will therefore need to be revisited after the collection, during the analysis.

5.2 CAPER data storage

- CAPER data can only be used for terrorism and serious crimes. The storage of CAPER data should be implemented in a separate repository. No contact with ordinary criminal databases should be allowed.

. Common criminality should use other databases. The reuse of CAPER data will be analysed in transfer of data.

. Time limit of retention is not a fixed period. In the e-communication, the Data Retention Directive has fixed a limit from 6 months to 2 years. Some data protection provisions for concrete EU LEAs have adopted a 5 years period as a limit. The USA in the PNR agreement has even obtained from the EU a 15 year period of retention of data.
The time period should be linked with the relevancy of the data. “No reason for storing irrelevant data or data that has become irrelevant” should be the rule.

- A good way of balancing the efficiency of serious crime and terrorism investigation and privacy would be to transform into dormant data the information after a 6 month period, for instance. The dormant data is a non-directly operational database guaranteed with anonymisation techniques and access restricted with authorisation.

. Special categories: sensible data should have specific rules on justification, access and reuse.

. Minors: added guaranties should be implemented for data about minors. Time limits retention should also be shorter.

- Information not needed in any investigation could be transferred to a non-operational third database (operational database, dormant data database, and now non-extracted information database), with non-extracted data. The access and reuse of these data about non-suspects should be extraordinarily limited, with due justification and explicit reference to the non use in any investigation.

5.3 CAPER data information management

- It is worth noting that CAPER is not an e-analysing tool, but an e-filter. This is important because CAPER data **are not analysed data**. No automatic decision should substitute the analysis of a human expert.

- CAPER data are row data. No classification of suspects, victims and witnesses can be automatically inferred from CAPER.. This should be clear if CAPER data are transferred. No indication of “analysed data” whatsoever should be given to CAPER data.

- Suspect, victims and witnesses are not CAPER data labels. They are the result of a human analysis on CAPER data.

- An information management process should transform CAPER data into labelled data ready to use for investigation.

Europol Information Management Process could be a model for Caper System.

The operational work at Europol ensures the maximum value of the use of information received from member states, through utilisation of the information management cycle. This cycle is the process of information collection, evaluation, collation, analysis and subsequent dissemination of an enhanced (information) product for investigative use within the member states. Enhanced information is the key with which to identify future deployment and direction of resources in the fight against serious organised crime.

One of the main benefits of information handling will be the ability to prioritise work. A well-defined process of the information flow will facilitate all the activities from the collection of relevant data towards a Europol product required by its final users.

Information management is a process based on raw information, be this on a crime, perpetrator, suspected person, etc. Raw information is evaluated and collated with other information received from various resources. Such information may then be examined or analysed to identify patterns or trends of criminal activity and finally disseminated to the member state that it affects. The security of information and data received at Europol is of vital importance. It is Europol's position that all data is evaluated and assigned a handling code before transmission to Europol. The product disseminated from Europol to member states will be encoded accordingly.

Evaluation and Handling Codes

Evaluation Codes

Evaluation codes are based on the 4x4 system used in the member states to establish the authenticity and accuracy of the supplied information. Evaluation codes consist of source codes and information codes.

Source Codes

A where there is no doubt of the authenticity, trustworthiness and competence of the source, or if the information is supplied by a source who, in the past, has proved to be reliable in all instances;
B source from which information received has in most instances proved to be reliable;
C source from which information received has in most instances proved to be unreliable;
X the reliability of the source cannot be assessed.

Information Codes

1 Information whose accuracy is not in doubt;
2 Information known personally to the source but not known personally to the official passing it on;
3 Information not known personally to the source but corroborated by other information already recorded;
4 Information which is not known personally to the source and cannot be corroborated.

The use of the 4x4 evaluation system is embodied in the analysis regulations as well as in the operational agreements Europol has signed with third parties

Handling Codes

Handling codes are both a complementary and necessary addition to evaluation codes in respect of information exchanged via Europol. Handling codes protect the information source, ensure future security of the information, and ensure that the information is processed in accordance with the wishes of the owner of the information.

The codes H1 and H2 are applied when the most common restrictions on the use of the information are applicable. H3 may be used to include additional restrictions, permissions and/or purpose of the transmission of the data.
The Handling Codes read as follows:

H1 This information must not be used as evidence in judicial proceedings without the permission of the provider.
H2 This information must not be disseminated without the permission of the provider.
H3 Other restrictions apply. The other restrictions, permissions and/or purpose of the transmission of the data should be described in free text.

Data Protection and Confidentiality

The purpose of data protection is to afford protection to the individual about whom data are processed. This is typically achieved through a combination of rights for the data subject and conditions for those who process data. Data protection within Europol is about creating a framework for Europol's information handling that appropriately takes care of the interests of the individual on whom law enforcement data are processed.
The level of protection of Europol information is a standardised format that indicates the protection measures that need to be applied to this information.
In this respect, three types of information can be identified:

• **(Europol) public information** = information which is marked or is clearly recognisable as being public information. The decision to allocate the public status to information can only be taken by head of unit or department within Europol, or a person under his authority, where the information originates;

• **Europol BPL information** = Basic Protection Level information (BPL);

• **Europol classified information** = information subject to a special security regime and marked with one of the classification levels: restricted, confidential, secret and top secret.

Sharing of information

There are two main tools at Europol to support the sharing of information: the Information System (IS) and the Information Exchange System (InfoEx).

The IS provides capabilities for storing, searching, visualising and linking information related to trans-national crimes, allowing law enforcement agencies across Europe to co-operate efficiently in their investigations. The system supports automatic detection of possible hits between different investigations and facilitates the sharing of sensitive information in a secure and reliable way.

Data can be inserted into the IS in a manual or automated way. The data inserted into the IS remain under the full control of the inputting party (data owner); they cannot be altered in any way by Europol or another member state. The owner is responsible for data accuracy, reliability and verification of storage time limits, and ensuring that they are kept up-to-date.

Data stored is only disseminated or used in accordance with the handling codes and Europol protection levels applied by the owner of the information.

The data in the IS are stored in different objects (persons, cars, identity documents...) which must be create a structured picture of a criminal case.

The exchange of information with Europol national units in the member states is secured via encrypted point-to-point lines. The third parties have an indirect access to this system through Europol's Information Management Operations Unit. The InfoEx provides four main functionalities: creation of a **Request**, creation of an **Answer**, **Search** engine and finally a catalogue of **Groups** to which requests may be addressed.

Operational Analysis

The Europol Analysis System (EAS) supports the work of Europol analysts. Direct access is permitted only to analysts working within specific analysis work files (AWFs). The system is dedicated to the analysis work files and has a number of specialist tools and software that facilitates a complete analysis of information supplied by the member states. The system is a vital tool in the processing and collation of information received from the member states.
The analysis work files contain clearly specified categories of persons (criminals, suspects, contacts, associates, victims, witnesses and informants) and data categories relevant to those persons, in accordance with the analysis work file regulations. The list of these categories is defined in a document known as the 'opening order'. Each analysis work file is unique in respect of the information that can be stored within it.

Analysis is a key element to Intelligence Led Policing. All analysis aims to "go beyond the facts". It takes incomplete and diverse data, collates it and tries to look at it in such a way that a new meaning can be seen from it, this can be to develop hypotheses or to identify intelligence gaps both of which allow the analyst to provide direction to the investigator. In this way it can be said that "added value" is given to the data.
To generalise, the analysis within an AWF is, according to the objectives and current focus, attempting to build up a picture of inter alia:

- Group structures;
- Individual roles;
- Modus operandi;
- Routes for commodities or money;
- Sequences of events.

This is not to be seen merely as an academic exercise by which the crime problem can be described. That description is a vital element towards understanding the scale and nature of the problem, and in turn it contributes towards identifying areas of vulnerability. In the end this is the key issue as it provides the best law enforcement opportunity. At a simpler level, by collecting diverse data from investigations throughout
the EU, the AWF is often able to link together seemingly insignificant details like the same telephone number appearing in the diary of different criminals by which separate investigations in different member states can be linked together.

Index System (IxS)

The Index System (IxS) provides a search function, which refers to the contents of the Europol Analysis System. It enables member states and Europol to determine if a subject of interest exists in any of the AWFs.

Who can access the Index System?

The Europol Director, the Deputy Directors and duly empowered officials of Europol and the member states' liaison officers can access the system.

What data can be retrieved from the Index System?

The data that can be retrieved refers to the contents of the Europol Analysis System. Access is defined in such a way that it is possible to determine whether or not a subject of interest is available in any of the AWFs, but it is not possible to establish connections or further conclusions regarding the content of the files.

5.4 CAPER data reuse and transfer

- CAPER data are not encoded or analysed data. Any transfer of CAPER data should warn on this important fact. Preferably, analysed data should be transferred and only CAPER data with specific indication of being raw data.

- CAPER transforms the former limitation of using data for only ONE CASE, erasing it afterwards. With tools like CAPER and their corresponding databases, more and more we have to think in ONE UNIQUE CASE, with concrete uses of a general unique network.

- In this context, purpose limitation is a key aspect: for serious crime and terrorism only.

- Other guarantees can be implemented in the sense that specific justification and authorisation are needed to access the CAPER data resulting network. The part of the network analysed will be restricted to what is needed in the case. The entire network will not be viewed and would require complementary and time limited authorisations.

- The reuse will require quality control on the CAPER data. The right to be informed, right to access and erase data is extraordinary limited within the terrorist and serious crime area. However, the CAPER data would be used for investigation and prosecution, after been analysed and determined the relevant data. The European Courts have started to held the possibility of a limited information right on the lawfully procedures to collect data used after in trials. Therefore, some legal validation of the procedure will be required to use it afterwards. Internal controls and independent controls should be implemented.

6 RECOMMENDATIONS (FIRST DRAFT)

Catalogue of Stored Data

Caper should have one clear and understandable list of the personal data to be stored.

Use of Clear Terms

LEA should be allowed to use or store data as long as the data are needed for the prevention, detection and investigation of terrorism and organised crime[84].

Pre-emptive data storing and the term "prevention of terrorism and organised crime" should be defined.

External and internal supervision

The existence of the prevention of terrorism and organised crime purpose should at any time be subject to external supervision.

A National Data Protection Authority or a EU common supervisory authority should also be a central access point for citizens.

An internal Data Protection body should be implemented, accompanied with rules that ensure its independency.

Access conditions

Access to CAPER database should be granted for the purpose of prevention, detection or investigation of terrorism or organised crime.

Explicit and detailed provisions with a list of allowed people to access should be adopted.

Access for consultation should be necessary in a specific case.

A reasoned written or electronic request should justify the reasons for access.

Any other request of access for other purposes should be rejected.

Improving the protection of Victims, Witnesses and people not guilty[85]

[84] Terrorist and serious crime offences could correspond to the offences in Articles 1 to 4 of Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism and Article 2(2) of Framework Decision 2002/584/JHA.
[85] BOEHME, F., Information *Sharing and Data Protection…, op.cit,* p. 402-404.

CAPER will include data of vulnerable people like victims, witnesses and people whose data have been preemptively stored based on factual indications (possible criminals). This could be considered indiscriminate data storing not tolerated by the European Court of Human Rights[86].

A step-by-step approach of those data should be applied: access should be permitted initially to only a few restrictive data, such as name, or date of birth and, if the search reveals a hit, further information could be provided later.

The data once marked by the human expert should maintain the label (victim, witness or possible criminal) and the step-by-step procedure. A data obviously could shift to another label (suspect) and then avoid this procedure.

When data of victims or witness are interlinked with other personal data, particular supervision should be provided to assure that the status of the person concerned would not be negatively influenced by the linking: a witness in an organised crime case and a person in a list to be refused entry.

Data should not be transferred to third parties. Only within the conditions of CAPER collaboration should these data be transferred. And the data should always be marked to keep the guarantee of the step-by-step procedure and particular supervision.

Individuals requesting access

Individuals should have the possibility to contact a EU supervisory body which then support them in exercising their access right.

The reasons to deny access should be clear and defined. Access can be denied when the access may jeopardise the fulfilment of the LEA tasks, or the rights and freedoms of third parties.

The application of the reasons to deny access should be open to external supervision. The external supervisory authority should have the possibility to access to the documents justifying the refusal. A time-limit of three months (for instance) to reply to an access should be implemented.

The right of information on the purpose of processing, the right to request rectification or deletion, the duration of the retention period, and the possibility to obtain assistance from the National Data Protection Authority or the Supervisory Authority could be limited. The notification could be withheld only in case the LEA activities were to be prejudiced.

Data security rules

It should be possible to verify what data have been entered and retrieved, when and by whom.

[86] *S. and Marper v. The United Kingdom*, Application nos. 30562/04 and 30566, Judgement of 4 December 2008..

The transferred data should be marked and the transmission recorded.

The supervisory authority should regularly check the admissibility of entering or retrieving the data.

Technical limitations of access should also be implemented to allow only authorised people to access the data. Privacy by design tools could help to limit abuses.

Time-Limits

A rule requiring the deletion of the data when particular circumstances are fulfilled would comply with the European Court of Human rights jurisdiction demanding a certain time-limit.

The storing may be extended when the data are used for ongoing investigations or ongoing analyses.

The supervisory body should be informed about and involved in cases when the original data storage period is extended.

Transmission to third parties

An agreement obliging the recipient to use the data only for the agreed purpose of transmission should be concluded before the transfer.

Data Protection Recommendations for the CAPER system	
Topic	Recommendations
1. Catalogue of Stored Data	• Caper should have one clear and understandable list of the personal data to be stored.
2. Use of clear terms	• LEA should be allowed to use or store data as long as the data are necessary for the prevention, detection and investigation of terrorism and organised crime[87]. • Pre-emptive data storing and the term "prevention of terrorism and organised crime" should be defined.
3. External and internal supervision	• The existence of the prevention of terrorism and organised crime purpose should at any time be subject

[87] Terrorist and serious crime offences could correspond to the offences in Articles 1 to 4 of Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism and Article 2(2) of Framework Decision 2002/584/JHA.

	to external supervision. • A National Data Protection Authority or an EU common supervisory authority should also be a central access point for citizens. • An internal Data Protection body should be implemented, accompanied with rules that ensure its independency.
4. Access conditions	• Access to CAPER database should be granted for the purpose of prevention, detection or investigation of terrorism or organised crime. • Explicit and detailed provisions with a list of allowed people to access should be adopted. • Access for consultation should be necessary in a specific case. • A reasoned written or electronic request should justify the reasons for access. • Any other request of access for other purposes should be rejected.
5. Improving the protection of Victims, Witnesses and people not guilty[88]	• CAPER will include data of vulnerable people like victims, witnesses and people whose data have been pre-emptively stored based on factual indications (possible criminals). This could be considered indiscriminate data storing not tolerated by the European Court of Human Rights[89]. • A step-by-step approach of those data should be applied: access should be permitted initially to only a few restrictive data, such as name, or date of birth and if the search reveals a hit, further information could be provided later.

[88] Boheme (2012, 402-404)
[89] *S. and Marper v. The United Kingdom*, Application nos. 30562/04 and 30566, Judgement of 4 December 2008.

	• The data once marked by the human expert should maintain the label (victim, witness or possible criminal) and the step-by-step procedure. A data obviously could shift to another label (suspect) and then avoid this procedure. • When data of victims or witness are interlinked with other personal data, particular supervision should be provided to assure that the status of the person concerned will not be negatively influenced by the linking: a witness in an organised crime case and a person in a list to be refused entry. • Data should not be transferred to third parties. Only within the conditions of CAPER collaboration should these data be transferred. And the data should always be marked to keep the guarantee of the step-by-step procedure and particular supervision.
6. Individuals requesting access	• Individuals should have the possibility to contact an EU supervisory body to support them in exercising their access right. • The reasons to deny access should be clear and defined. Access can be denied when the access may jeopardise the fulfilment of the LEA tasks, or the rights and freedoms of third parties. • The application of the reasons to deny access should be open to external supervision. The external supervisory authority should have the possibility to access to the documents justifying the refusal. A time-limit of three months (for instance) to reply to an access should be implemented. • The right of information on the purpose of processing, the right to

	request rectification or deletion, the duration of the retention period, and the possibility to obtain assistance from the National Data Protection Authority or the Supervisory Authority could be limited. The notification could be withheld only in case the LEA activities are to be prejudiced.
7. Data security rules	• It should be possible to verify what data have been entered and retrieved, when and by whom. • The transferred data should be marked and the transmission recorded. • The supervisory authority should regularly check the admissibility of entering or retrieving the data. • Technical limitations of access should also be implemented to allow only authorised people to access the data. Privacy by design tools could help to limit abuses.
8. Time-Limits	• A rule requiring the deletion of the data when particular circumstances are fulfilled would comply with the European Court of Human rights jurisdiction demanding a certain time-limit. • The storing may be extended when the data are used for ongoing investigations or ongoing analyses. • The supervisory body should be informed about and involved in cases when the original data storage period is extended.
9. Transmission to third parties	• An agreement obliging the recipient to use the data only for the agreed purpose of transmission should be concluded before the transfer.

7 CONCLUSIONS

7.1 Legal scenarios

There is no ready-to-use General Data Protection Framework on organised crime for the CAPER project. On the contrary, the patchwork of data protection rules leads to a situation in which the former EU pillar structures still have a great importance.

Nonetheless, the impact of the Lisbon Treaty may lead to a future data protection framework. One of the problems is the restricted scope of the main legal rules now in force, i.e. the Directive 95/46, the Regulation 45/2001 and the Council Framework Decision. Moreover, there is a lack of principles for data protection and organized crime investigations through EU case-law. Nevertheless, some case law like *Huber v. Germany* in the former first pillar show the willingness of the EU Courts to establish such a data protection regime beyond the former third pillar structure. This tendency needs to be confirmed in future rulings.

The Council Framework Decision, with its vague provisions and broad exemptions is not ruling satisfactorily organised crime as a General Data Protection Framework should do (Boheme, 2012, 171-173).[90]

The limits of the Council Framework Decisions are:

- The purpose limitation principle is so weak that authorities processing the data can decide about the change of the purpose;
- Guarantees of adequacy of data, time limits, protection of sensitive data, updating of information and right to get access to data are formulated in a mitigated way;
- The obligation to notify the individuals about the data processing is not compulsory and is left to the discretion of the state members;
- There is no right to object;
- Far reaching derogations for Member States for data transfering to third states;
- Access by LEAs to data stored in private databases is not regulated.

Therefore, there is no specific data protection framework for the common foreign and security policy domain. According to Article 39 TEU there will be future data protection rules in this area. The Court of Justice provided some indications in the so called terrorist blacklists, and settled complementary rights like the right to defence and judicial protection.

To sum up, the Council Framework Decision data protection guarantees are less strict than the Directive and 45/2001 Regulation provisions. Its restricted scope also limits the application of the Council Framework Decision in the AFSJ area. As a result, data protection in the AFSJ area is left to legal tools establishing the AFSJ actors. They were quickly enacted before the entry in force of the Lisbon Treaty to avoid the wide application of general data protection, according to Article 16 TFEU.

90

We do not know yet whether the 2012 Data Protection Reform will be the Data Protection General Framework on organised crime and terrorism we are expecting to. The European Data Protection Supervisor and the Article 29 Data Protection Group have reliesed interesting reports on this open issue. Last December 17th, a second alternate Draft was laid down by the European Parliament's rapporteur Jan Philipp Albrecht (Committee for Civil Liberties, Justice and Home Affairs / LIBE). This is an unusual situation, to be gentle, showing a tough political debate behind the law. Further analyses on later versions of legal tools will be added in future Deliverables.

7.2 Ethics and the CAPER Regulatory Model (CRM)

Within this complex legal maze, computer ethics and regulatory models come to play. Law, moral principles and governance are deeply entrenched.

In this Deliverable (i) we answered the questions posed by the members of the Ethical Committee in his first evaluation; (ii) we described the state of the art of informational ethics, computer ethics, ethical codes and other regulatory tools; (iii) we advanced a structured scheme to bring together relevant elements from the legal, political and ethical fields (hard law, soft law, governance, and best practices); (iv) we explained how the CRM can be consistently built bringing into it some principles and values from Privacy by Design, Linked Open Data and Security by Design; (v) we described the conceptual nature of the CRM and how specific recommendations could be triggered out of it; (vi) we clarified the difference between Impact Assessment (IA), Privacy Impact Assessment (PIA) and Data Protection Impact Assessment (DPIA); (vii) we set up specific risk scenarios to test possible solutions; (viii) finally, we made the proposal of two sets of Recommendations to be discussed with partners and LEAs and to be evaluated by the Ethical Committee.

The best way to offer regulatory advice and tools to CAPER is, in our opinion, following the empirical track pointed out by PIAs and DPIAs experiences. It is our contention that being stuck down to earth, to the specific questions and problems faced by partnes and LEAs, is a good way to start discussing how to rule the construction, management and eventual use of the platform as a Web service.

We have also divided all the activities related to the use of CAPER tools into four successive stages: (i) profiling, (ii) storage, (iii) management (iv) and transfer to third parties. We have only mentioned several options to be discussed with LEAs, technical partners and members of the Ethical Committee, in order to set in future Deliverables fuller risk scenarios and data protection preserving solutions for CAPER.

8 REFERENCES

Arai-Takahashi, Y. (2002). *The margin of appreciation doctrine and the principle of proportionality in the jurisprudence of the ECHR*, Antwerp: Intersentia.

Albrecht, J.P. (2012). "General Data Protection Regulation in 10 Points. From a Directive to Regulations." Document 20 December. http://www.janalbrecht.eu/uploads/pics/data_protection_English.pdf

Austill, A.D. (2011). "Legislation Cannot Replace Ethics in Regulatory Reform", *International Journal of Business and Social Science* 2 (13) [Special Issue - July]: 61-71.

Aycock, J.; Sullins, J. Ethical (2010). "Proactive Threat Research", R. Sion et al. (Eds.), *FC 2010 Workshops*, LNCS 6054, Berlin, Heidelberg, IFCA/Spriger, pp. 231–239.

Bainbridge, D. (2005). *Data protection*, St. Albans: xlp publishing.

Balogava. L. (2008). "The developments in the case law of the community courts with regard to OLAF investigations". *Eurcrim* 3–4: 142–145.

Balzacq T., Bigo D., Carrera S., Guild E. (2006). "Security and the two-level game: the treaty of Prüm, the EU and the management of the threats", Centre for European Policy Studies (CEPS) working paper, published 1 January 2006. Accessible at: http://www.ceps.eu/book/securityand-two-level-game-treaty-pr%C3%BCm-eu-and-management-threats.

Beattie, K. (2009). "S. and Marper v UK: privacy, DNA and crime prevention", *Eur Hum Rights Law Rev* 2: 229–238.

Beck, G. (2008). "Human rights adjudication under the ECHR between value pluralism and essential contestability", *Eur Hum Rights Law Rev* 2: 214–244.

Becker, L. (2012). "Design and Ethics: Sealed-Off Thinking", *Interactions* 19 (2): 51-53.

Boehm, F. (2012). *Information Sharing and Data Protection in the Area of Freedom, Security and Justice*, Springer-Verlag Berlin Heidelberg: Springer Verlag.

Bondy, K.; Matten, D.; Moon, J. (2006). "MNC codes of conduct: CSR or corporate governance?", International Centre for Corporate Social Responsibility, Research Paper Series, No. 40-2006, pp. 1-28, available at: www.nottingham.ac.uk/business/ICCSR

Brouwer, E. (2008). *Digital borders and real rights – effective remedies for third-country nationals in the Schengen information System*. Leiden: Martinus Nijhoff.

Brouwer, E. (2008). *The other side of moon – the Schengen information system and human rights: a tasks for national courts*. Centre for European Policy Studies, CEPS Working Document No. 288 of April 2008.

Bunge, M. (1996). *Ética, ciencia y técnica*, Buenos Aires: Ed. Sudamericana.

Burmeister-Lamp, K.; Lévesque, M. ; Schade, C. (2012). “Are entrepreneurs influenced by risk attitude, regulatory focus or both? An experiment on entrepreneurs' time allocation”, *Journal of Business Venturing*, 27 (2012): 456–476.

Cali, F. (2000). “Europol’s data protection mechanisms: what do they know and whom are they telling?”, *Touro Int Law Rev* 10: 189–238.

Cameron, I. (2000). *National security and the European convention on human rights*, The Hague: Kluwer Law International.

Cameron, Kim (2005). *The Laws of Identity* …as of 5/11/2005. Microsoft Corporation.

Capurro, R.; Britz, J.B. (2010). “In search of a code of global information ethics: The road travelled and new horizons”, *Ethical Space: The International Journal of Communication Ethics*, 7 (2/3): 28-36.

Carey, P. (2004). *Data protection: a practical guide to UK and EU law*. Oxford: Oxford University Press.

Casanovas, P. (2013) “Agreement and Relational Justice: A Perspective from Philosophy and Sociology of Law”, in S. Ossowski (Ed.) *Agreement Technologies*, LGT Series 8, Springer Verlag, Heidelberg, Dordrecht, 2013, pp. 17-42.

Cavoukian, A. (2006). “7 Laws of Identity: The Case For Privacy-Embedded Laws of Identity in the Digital Age”, *Technology*, Ontario Information and Privacy Commissioner, October 2006, 1-24.

Cavoukian, A. (2010). “Privacy by Design. The 7 Foundational Principles. Implementation and Mapping of Fair information Practices. Information an Privacy Commissioner, Ontario, Canada, 2010.

Cavoukian, A.; Jonas, J. (2012) “Privacy by Design in the Era of Big Data”, June 8, 2012, http://privacybydesign.ca/content/uploads/2012/06/pbd-big_data.pdf (accessed 30/11/2012).

Christou, V. (2008). “The Council decision of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II)”, *Columbia J Eur Law*: 649–657, Summer 2008.

Clarke, R. (1988). “Information Technology and Dataveillance”, *Commun. ACM* 31 (5): 498-512, re-published in C. Dunlop and R. Kling (Eds.), *Controversies in Computing*, Academic Press, 1991.

Clarke, R. (2011). “An Evaluation of Privacy Impact Assessment Guidance Documents”, *International Data Privacy Law*, 1 (2): 111-120. Pre-print: http://www.rogerclarke.com/DV/PIAG-Eval.html

Coninsx, M., da Mota J.L. (2009). “The international role of Eurojust in fighting organised crime and terrorism”, *Eur Foreign Aff Rev* 14:165–169.

Crank, J.P; Gregor, P.E. (2005). *Counter-Terrorism After 9/11: Justice, Security and Ethics Reconsidered*, LexisNexis.

Cranor, L.F. (2010). "Ethical Concerns in Computer Security and Privacy Research Involving Human Subjects", R. Sion et al. (Eds.), *FC 2010 Workshops*, LNCS 6054, 2010, Springer-Verlag Berlin Heidelberg: 247–249.

Cullen, P., Jund, S. (2002). *Criminal justice co-operation in the European Union after Tampere*. Bundesanzeiger, Köln: Series of Publications by the Academy of European Law in Trier.

Curtis, G. E. (2008). "Legal and Regulatory Environments and Ethics: Essential Components of a Fraud and Forensic Accounting Curriculum", *Issues in Accounting Education* 23 (4) (2008): 535-543.

Davis, M. (2001). "Three Myths about Codes of Engineering Ethics", *IEEE Technology and Society Magazine*, 20 (3): 8-16.

Davis, M. (1991). (1991). "Do cops really need a code of ethics?" *Criminal Justice Ethics*, Summer/Fall 10 (2): 1-15.

De Buck, B. (2007). "Joint investigation teams: the participation of Europol officials", *ERA Forum* (8): 253–264.

De Busser, E. (2009). *Data protection in EU and US criminal cooperation*. Antwerpen: Maklu.

De Hert P., Guthwirth S. (2006) "Privacy, data protection and law enforcement. Opacity of the individual and transparencs of power". In: Cleas E, Duff A, Gutwirth S (eds) Privacy and the criminal law. Intersentia, Antwerpen, pp. 61–104.

De Hert. P.; Gutwirth, S. (2006). "Interoperability of police databases within the EU: an accountable political choice?", *Int Rev Law Comput Technol* 20 (1&2): 21–35.

De Hert, P.; Gutwirth, S. (2009) "Data protection in the case law of Strasbourg and Luxembourg: constitutionalisation in action", in *Reinventing data protection*, Springer, Heidelberg, pp. 3–44.

De Hert, P.; Schreuders, E. (2001). Report "The relevance of Convention 108", in *Proceedings of the Council of Europe Conference on Data Protection*, Warsaw, 19–20 November 2001.

De Hert, P.; Vandamme, L. (September 2004). "European police and judicial information-sharing, cooperation: incorporation into the community, bypassing and extension of Schengen", *ERA Forum* 5 (3): 425–434.

De Hert, P. (2005). *Biometrics: legal issues and implication – background paper for the Institute of prospective Technological Studies*. DG JRC, Sevilla, European Commission, January 2005.

De Hert, P.; Bellanova, R. (2008.) "Data protection from a transatlantic perspective: The EU and US move towards an international data protection agreement?", study requested by the

European Parliament's Committee on civil liberties, justice and home affairs (LIBE), pp. 25–26 and 37–38.

De Hert, P. (2012). "A Human Rights Perspective on Privacy and Data Protection Impact Assessments", in Wright, D., de Hert, P. (Eds.) *Privacy Impact Assessment*, LGTS n. 6, Berlin, Dordrecht, N.Y.: Springer Verlag, pp. 33-76.

De Moor A.; Vermeulen, G. (2010). "The Europol council decision: transforming Europol into an agency of the European Union", *Common Market Law Rev* 47 (4): 1089–1121.

De Moor, S. (2009). "The difficulties of joint investigation teams and the possible role of OLAF", *Eucrim* 3: 94–99.

De Schutter, O. (2008). "The two Europes of human rights: the emerging division of tasks between the Council of Europe and the European Union in promoting human rights in Europe", *Columbia J Eur Law* 14: 509–560.

De Vries, K.; Bellanova, R.; de Hert, P. (2010). Proportionality overrides unlimited surveillance, the German constitutional court judgment on data retention. Centre of European Policy Studies, Liberty and Security in Europe. Available at: http://www.ceps.eu/book/proportionalityoverrides-unlimited-surveillance.

Den Boer, M.; Hillebrand. C.; Nölke, A. (2008). "Legitimacy under pressure: the European web of counter-terrorism networks", *JCMS* 46 (1):101–124.

De Simone, C. (2010). "Pitting Karlsruhe against Luxembourg? German data protection and the contested implementation of the EU data retention directive", *German Law J* 11 (3): 291–318.

Dittrich, D.; Bailey, M.; Dietrich, S. (2011). "Building an Active Computer Security Ethics Community", *IEEE Computer and Reliability Societies*, July/August, 32-40.

Duncan, J.F. (2011). *Ethical Design for Security and Privacy*. Doctoral Dissertation. School of Informatics and Computing, Indiana University, April, UMI 3456457.

Ekenberg, L.; Oberoi, S.; Orci, I. (1995). "A cost model for managing information security hazards", *Computers & Security*, 14: 707-717.

Everett, Bernard. (2912). "The encryption conundrum", *Network Security*, April: 15-18.

Farrell, B.J.; Cobbin, D.M.; Farrell, H.M. (2002). "Codes of ethics: Their evolution, development and other controversies", *Journal of Management Development*, 21 (2): 152 – 163.

Floridi L. (2006). "The Ontological Interpretation of Informational Privacy", *Ethics and Information Technology*, 7(4): 185–200.

Foster, G.E. (2001). "Ethics, Governement, and Security, the moral imperative", *The Humanist*, May/June: 6-8.

Galison, P. (1994). "The Ontology of the Enemy: Norbert Wiener and the Cybernetic Vision", *Critical Inquiry*, 21 (1): 228-266.

Garside, A. (2006). "The political genesis and legal impact of proposals for the SIS II: what cost for data protection and security in the EU?" Sussex Migration Working Paper no. 30, March, p. 16. Accessible at: http://www.sussex.ac.uk/migration/documents/mwp30.pdf.

Geyer F (2008). "Taking stock: databases and systems of information exchange in the area of freedom, security and justice", published 6 May, Centre for European Policy Studies, research paper No. 9. Available at: http://shop.ceps.eu/book/taking-stock-databases-andsystems-information-exchange-area-freedom-security-and-justice.

Gino, F.; Margolis, J.D. (2011). "Bringing ethics into focus: How regulatory focus and risk preferences influence (Un)ethical behaviour", *Organizational Behavior and Human Decision Processes* 115: 145–156.

Gonzalez Fuster, G.; de Hert P; Ellyne, E.; Gutwirth, S. (2010). "Huber, Marper and others: throwing new light on the shadows of suspicion", CEPS working paper, Centre for European Policy Studies, No. 8/June, p. 2. Accessible at: http://www.ceps.eu/book/huber-marper-andothers-throwing-new-light-shadows-suspicion.

Gonzalez-Herrero, J. (2009). "The collection of evidence by OLAF and its transmission to the national judicial authorities", *Eucrim* 3: 90–94.

Gravitz, M.A. (2009). "Professional Ethics and National Security: Some Current Issues", *Consulting Psychology Journal: Practice and Research*, 61 (1): 33–42.

Greenwald, S.J. (Panel Chair/Editor); D. Snow, B.D.; Ford, R.; Thieme, R. (2008). "Towards an Ethical Code for Information Security?", *NSPW'08,* September 22–25. Lake Tahoe, California, ACM, 75-87.

Greer, S. (2006). *The European convention on human rights, achievements, problems and prospects*. Cambrige: Cambridge University Press.

Griller, S.; Orator, A. (February 2010). "Everything under control? The "way forward" for European agencies in the footsteps of the Meroni doctrine", *Eur Law Rev* 35 (1): 3–35.

Groussot, X.; Popov, Z. (2010). "What's wrong with OLAF? Accountability, due process and criminal justice in European anti-fraud policy", *Common Market Law Rev* 47 (3): 605–643.

Gualtiere, C. (2007). "Joint investigation teams", *ERA Forum* (8): 233–238.

Guild, E. (2008). "The uses and abuses of counter-terrorism policies in Europe – the case of the terrorist lists", *J Common Market Stud* 1: 173–193.

Gutwirth, S. (2002). *Privacy and the information age*. Boston: Rowman & Littlefield.

Hamilton, A.; Jay, R. (2003). *Data protection: law and practice*. London: Sweet & Maxwell.

Harbert, T. (2007). "Dark Secrets, Ugly Truths. And Little Guidance", 34 *Computerworld*, October 29: 35-37.

Hedgecoe, A. (2012). “Trust and Regulatory Organizations: the Role of Local Knowledge and Facework in Research Ethics Review”. *Social Studies of Science,* published online 13 June, *Social Studies of Science* 0(0) 1–22.

Helmberg, M. (2007) “Eurojust and joint investigation teams: how Eurojust can support JITs”, *ERA Forum* 8: 245–251.

Heusel, W. (2002). *The charter of fundamental rights and constitutional development in the EU.* Bundesanzeiger, Köln: Schriftenreihe der Europäischen Rechtsakademie Trier.

Hijmanns, H. (2010). “Recent developments in data protection at European Union level”, *ERA Forum* 2 (11): 219–231.

Hijmanns, H.; Scirocco, A. (2009). “Shortcomings in EU data protection in the third and the second pillars. Can the Lisbon Treaty be expected to help?”, *Common Market Law Rev* 46: 1485–1525.

Hijmans, H. (2006). “The European data protection supervisor: the institutions of the EC controlled by an independent authority”, *Common Market Law Rev* 43: 1313–1342.

Hofmann, H.C.H; Rowe, G.C.; Turk, A.H. (2011). *EU administrative law and policy of the European Union*. Oxford: Oxford University Press.

Hollis, S. (2010). “The necessity of protection: Transgovernmental networks and EU security governance”, *Cooperation and Conflict* 45 (3): 312–330.

Horvatis L.; de Buck, B. (2007). “The Europol and Eurojust project on joint investigation teams”, *ERA Forum* 8: 239–243.
http://cybersecurity.jrc.ec.europa.eu/docs/LIBE%20Biometrics%20March%2005/LegalImplications_Paul_de_Hert.pdf.

Humphreys, E. (2008). “Information security management standards: Compliance, governance and risk management”, *Information Security Technical Report* 13: 247-255.

Hunter, R.E.; Gnehm, E.; Joulwan, G.; Chivvis, C. (Rapporteur) (2008). *Integrating Instruments of Power and Influence Lessons Learned and Best Practices*, RAND Corporation, National Security Report Division, 109 pp.

Jensen, T.; Sandström, J.; Helin, S. (2009) “Corporate Codes of Ethics and the Bending of Moral Space”, *Organization* 16: 529-545.

Jonas, J. (2012a). “G2 | Sensemaking – One Year Birthday Today. Cognitive Basics Emerging.”, January 28, http://jeffjonas.typepad.com/jeff_jonas/2012/01/g2-sensemaking-1-year-birthday-today-cognitive-basics-emerging.html (accessed 30/11/2012).

Jonas, J. (2012b). “Privacy by Design in the Era of Big Data”, June 18, 2012, http://jeffjonas.typepad.com/jeff_jonas/2012/06/privacy-by-design-in-the-era-of-big-data.html (accessed 30/11/2012).

Jonas, J. (2012c). “Fantasy Analytics”, November 9, http://jeffjonas.typepad.com/jeff_jonas/2012/11/fantasy-analytics.html(accessed 30/11/2012).

Kay, S. (2004). “Globalization, Power, and Security”, *Security Dialogue* Vol. 35 (1): 9–25.

Kenneally, E.; Bailey, M.; Maughan, M. (2010). “A Framework for Understanding and Applying Ethical Principles in Network and Security Research”, in R. Sion et al. (Eds.) *FC 2010 Workshops*, LNCS 6054, IFCA/Springer-Verlag Berlin Heidelberg (2010), pp. 240-46.

Knighton, T. (2004). “The 'a capella' Heresy in Spain: An Inquisition into the Performance of the 'cancionero' Repertory”, *Early Music*, Vol. 20, No. 4, Iberian Discoveries I (Nov., 1992): 560-581.

Kritzinger, E.; von Solms, S.H. (2006). “E-learning: Incorporating Information Security Governance”, *Issues in Informing Science and Information Technology*, 3: 319-325.

Kuner, C. (2009). “An international legal framework for data protection: issues and prospects”, *Computer Law Security Rev* 25: 307–317.

Ladenburger, C. (2008). “Police and criminal law in the Treaty of Lisbon – a new dimension for the community model”, *Eur Constitut Law Rev* 4 (1): 20–40.

Lenaerts, K. (2010). “The contribution of the European Court of justice to the area of freedom, security and justice”, Int Comp Law Q 59: 255–301.

Lischka, K.; Stöcker, C. (2013). “Data Protection: All you need to know about the EU Privacy Debate”, Der Spiegel Online, January 18. http://www.spiegel.de/international/europe/the-european-union-closes-in-on-data-privacy-legislation-a-877973.html

Lloyd, P. (2009). “Ethical imagination and design”, Design Studies 30: 154-168.

Lopes da Mota, J.L. (2009). “Eurojust and its role in joint investigation teams”, *Eucrim* (3): 88–90.

Manolea, B. (2010). “Implementation of EU data retention directive unconstitutional”, *Computer Law Rev Int* 2: 49–51.

Maras, M-H. (2009). “From targeted to mass surveillance: is the EU Data Retention Directive a necessary measure or an unjustified threat to privacy?”, in *New direction in surveillance and privacy*, Willan Publishing, Cullompton, pp. 74–103.

Matwyshyn, A.; Cui, Ang; Keromytis, A.D.; Stolfo, S. J. (2010). “Ethics in Security Vulnerability Research”, *IEEE Computer and Reliability Societies*, March/April, pp. 67-71.

Mcdonald, G.M. (2009). "An anthology of codes of ethics", *European Business Review*, 21 (4): 344 – 372.

McGuinness, S. (2008). “Research Ethics Committees: The Role of Ethics in a Regulatory Authority”, *Journal of Medical Ethics*, 34 (9): 695-700.

McNutt, P.A.; Batho, C.A. (2005). "Code of ethics and employee governance", *International Journal of Social Economics*, 32 (8): 656 – 666.

Mendez, M. (2007). "Passenger name record agreement, European court of justice", *Eur Constitut Law Rev* 3: 127–147.

Papakonstantinou, V.; De Hert, P. (2009). "The PNR agreement and transatlantic anti-terrorism cooperation: no firm human rights framework on either side of the Atlantic", *Common Market Law Rev* 46 (3): 885–919.

Parker, D. "(Regulatory) Impact Assessment and Better Regulation", in D. Wright and P. de Hert (Eds.), *Privacy Impact Assessment*, LGT Series 7, Heidelberg, Dordrecht, Springer Verlag, pp. 79-96.

Payne, D.; Landry, B.J.L. (2006). "A Uniform Code of Ethics: Business and IT Professional Ethics", *Communications of the ACM*, 49 (11): 81-84.

Raab, Ch.; Wright, D. "Surveillance: Extending the Limits of Privacy Impact Assessment" , in D. Wright and P. de Hert, *Privacy Impact Assessment*, LGTS n. 6, Berlin, Dordrecht, N.Y.: Springer Verlag, 2012, pp. 363-383.

Rallo Lombarte, A. "The Madrid Resolution and Prospects for Transnational PIAs"**,** , in D. Wright and P. de Hert, *Privacy Impact Assessment*, LGTS n. 6, Berlin, Dordrecht, N.Y.: Springer Verlag, 2012, pp. 385-396.

Rijken, C. (2006). "Joint investigation teams: principles, practice and problems, lessons learnt from the first efforts to establish a JIT", *Utrecht Law Rev* 2 (2): 99–118.

Rijken, C.; Vermeulen, G. (2006). "Joint investigation teams in the European Union, from theory to practice", The Hague: T.M.C Asser Press.

Salminen, A. (2010). *Ethical Governance*, Helsinki: Vaasan Ylioplisto.

Scirocco, A. (2008). "The Lisbon Treaty and the protection of personal data in the European Union". No. 5 February. Available at: http://www.dataprotectionreview.eu/.

Shockwave Writer. (2002). "Ethics, Professionalism and Protecting Assets", *Computer, Fraud and Security*, 31 May, 5: *17–19*.

Siponen, M.; Willison, R. (2009). "Information security management standards: Problems and solutions", *Information & Management* 46: 267–270.

Snow, B.; Brooks, B. (2009). "Privacy and Security: An Ethics Code for U.S. Intelligence Officers", *Communications of the acm*, August, 52 (8): 30-32.

Somers, M.J. (2001). "Ethical Codes of Conduct and Organizational Context: A Study of the Relationship Between Codes of Conduct,Employee Behavior and Organizational Values", *Journal of Business Ethics* 30: 185–195.

Spafford, E.H. (2010). "Security, Technology, Publishing, and Ethics (Part I)" http://dx.doi.org/10.1016/j.cose.2010.10.004 *Computers & Security* 29: 813 -814.

Spafford, E.H. (2011). “Security, Technology, Publishing, and Ethics (Part II)” *Computers & Security* 30: 2-3.

Staicu, A. (2008). “The future of OLAF – legal framework and the proposal for a regulation amending the OLAF regulation”, EUCRIM (3–4): 177–180.

Staicu, A.; Vervaele, J.; Kuhl, L. (2008). “OLAF’s future role and the European public prosecutor”, *Eucrim* 3–4:177–192.

Turilli, M. (2007). “Ethical Protocols Design”, *Ethics and Information Technology* 9: 49–62.

Uthmani, O.; Buchanan, W.; Lawson, A.;Thuemmler, C.; Supt. Scott, R.; Lavery, A.; Mooney, C. (2010). “Novel Information Sharing Syntax for Data Sharing between Police and Community Partners, using Role-based Security”, *The 9th European Conference on Information Warfare and Security* held at the Department of Applied Informatics, University of Macedonia, Thessaloniki, Greece. 1-2 July, n. 3819, http://researchrepository.napier.ac.uk/id/eprint/3819.

Vervaele, J.A.E. (2008). “The shaping and reshaping of Eurojust and OLAF”, *Eucrim* 3–4: 180–186.

von Solms, B. 2005. “Information Security governance: COBIT or ISO 17799 or both?”, *Computers & Security* 24: 94-104.

von Solms, B.; von Solms, R. (2004). “The 10 deadly sins of information security management”, *Computers & Security* 23: 371-376.

Vroom, C.; von Solms, R. (2004). “Towards information security behavioural compliance”, *Computers & Security* 23:191-198.

Walker, N. (2004). *Europe’s area of freedom, security and justice*, Oxford: Oxford University Press.

Wallwork, A.; Baptista, J. (2005). “Unterstanding interoperability”, in Backhouse, J. (ed.) *Structured account of approaches on interoperability*, Chap 4, D4.1. Future of Identity in the Information Society (FIDIS), 6th Framework Programme, EU Commission, published 12 July 2005, pp. 19–28. Available at: http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp4-del4.1.account_interoperability.pdf.

Wickham, M.; O’Donohue, W. (2012). “Developing an Ethical Organization: Exploring the Role of Ethical Intelligence”, *Organization Development Journal*, 30 (2): 9-30.

Wiener, N. (1950). *The Human Use Of Human Beings: Cybernetics and Society*, DaCapo Press, Boston: DaCapo Press, with Houghton Mifflin Co. 1954.

Wright, D.; Wadhwa, K.; de Hert, P.; Kloza, D. (2011). *A Privacy Impact Assessment Framework for data protection and privacy rights,* Deliverable 1, PIAF, 2009-2010/DAP/AG, JLS/2009.

Wright, D. (2012). "(Regulatory) Impact Assessment and Better Regulation", in *Privacy Impact Assessment*, LGTS n. 6, Berlin, Dordrecht, N.Y., Springer Verlag, pp. 77-96.

Wright, D; de Hert, P. (2012). "Introduction to Privacy Impact Assessment", in *Privacy Impact Assessment*, LGTS n. 6, Berlin, Dordrecht, N.Y., Springer Verlag, pp. 3-32.

Wright, D., de Hert, P. (Eds.). (2012). *Privacy Impact Assessment*, LGTS n. 6, Berlin, Dordrecht, N.Y., Springer Verlag.

Wright, D.; Mordini, E. (2012). "Privacy and Ethical Impact Assessment", in *Privacy Impact Assessment*, LGTS n. 6, Berlin, Dordrecht, N.Y.: Springer Verlag, pp. 397-418.

9 ANNEXES/DOCUMENTS

9.1 Codes of Ethics

9.1.1 Codes

ACM Code of Ethics and Professional Conduct http://www.acm.org/about/code-of-ethics (*Adopted by ACM Council 10/16/92)*

Computer Ethics Institute. *Ten Commandments for Computer Ethics*. http://computerethicsinstitute.org/publications/tencommandments.html

Ethics Working Group. http://ethics-wg.org/, Ethics Committee Overview Presentation (PPT), Ethics Review Policy

IEEE Code of Ethics http://www.ieee.org/about/corporate/governance/p7-8.html

ISSA *Code of Ethics*

ISSA *Generally Accepted Security Principles* (GAISP) v.3.0. (2004)

ISSA Information Systems Security Association (ISSA). *Policies and Procedures. Operations Manual.*

(ISC)^2 Overview. *Evolving in Today's Complex Security Landscape*

ISC)² *Code Of Ethics* . Ethics Complaint Procedures, Universal Ethics Workgroup https://www.isc2.org/ethics/default.aspx

UNESCO. *Code of Ethics or the Information Society*, proposed by the Intergovernmental Council of the Information for all Programme (IFAP), 18th session, held in February 2011, 36C/49.

9.1.2 Code of Ethics for the Information Society (UNESCO, 2011)

1. Internet in particular and ICTs more generally should be recognized as a key public service for building a people-centred, inclusive and development-oriented information society and are crucial to promote the exercise and enjoyment of universally recognised human rights and fundamental freedoms.
2. Every person irrespective of where they live, their gender, education, religion, social status shall be able to benefit from the Internet and use of ICTs. Everyone shall be able to connect, access, choose, produce, communicate, innovate and share information and knowledge on the Internet.
3. Affordable access to the Internet should serve as a tool for development, social cohesion and for enabling everyone's potentials. Active social participation in public life through the use of Internet and other ICTs shall be enabled on a non-discriminatory basis.
4. Information should be made available, accessible and affordable across all linguistic, cultural and social groups and to both genders, including people with physical, sensory or cognitive disabilities, and people who speak minority languages. Internet and other ICTs

shall serve to reduce digital divide and deploy technology and applications to ensure inclusion.
5. Technological and methodological standards, access solutions, portability and interoperability shall allow the widest possible access to content and content production, and encourage the evolution and improvement of the Internet and other ICTs to bring about greater inclusion and overcome forms of discrimination.
6. Creation, preservation and processing of, and access to, educational, cultural and scientific content in digital form should be encouraged, so as to ensure that all cultures can express themselves and have access to Internet in all languages, including indigenous and minority languages.
7. Everyone should have a freedom of association on the Internet and ICT-mediated assembly. Member States should take preventive steps against monitoring and surveillance of assembly and association in a digital environment.
8. Member States and respective stakeholders should take all steps to develop trustworthy Internet and other ICTs ensuring security, reliability and stability of critical and pervasive applications and services.
9. Member States should encourage and extend the availability of information in the public domain, recognize and enact the right of universal online access to public and government-held records, including information relevant to citizens. Publicly-relevant information should be placed in the public domain and disseminated online in an easily accessible way using compatible and open formats.
10. Media and information literacy is a fundamental prerequisite for access to information, the exercise of cultural rights and the right to education through use of Internet and other ICTs. It is essential to ensure that all user groups have the knowledge and skills to act and make informed and clear consent-based choices using Internet and ICTs so that they can be fully responsible members of the information society.
11. Everyone has a right to freedom of expression, participation and interaction on the Internet that should not be restricted, except in those narrowly defined circumstances that are based on internationally recognized laws and universal human rights standards.
12. Everyone has a right to the protection of personal data and private life on the Internet and other ICTs. Users should be protected against the unlawful storage, abuse or unauthorized disclosure of personal data, and against the intrusion of their privacy.
13. All stakeholders shall work together to prevent against abusive uses of ICTs, protection of private data and privacy and violation of human rights on the Internet and other ICTs by combination of legislative measures, user education, including use of media and information literacy skills, self-regulation and co-regulation measures and technical solutions without disrupting the free flow of information.
14. Member States should implement preventive measures and coordinate strategies to ensure security on the Internet and the protection of society against cybercrime, including acts motivated by racism, racial discrimination, xenophobia and related intolerance, hatred, violence, all forms of child abuse, and trafficking and exploitation of human beings.
15. All members of the information society, either collective or individual, should be free to develop and distribute new content and applications on the Internet. Freedom of expression and creative use of ICTs should not be restricted, except when impinging upon the basic human rights of others. The basic technical standards used on the Internet and other ICTs must always be open to allow interoperability and innovation.
16. Member States should support the use of the Internet and other ICTs to enhance the effectiveness of democracy and democratic institutions, providing to the public opportunities for effective public deliberation and participation in democratic process, and promoting transparency, accountability, responsiveness, engagement, inclusiveness, accessibility, participation, subsidiary and social cohesion.

17. Intellectual property of the creations in a digital environment should be a subject of and shall be protected under the intellectual property rights legislation. Unauthorized copying and distribution of copyrighted materials must not be condoned. Legal frameworks facilitating owners of intellectual property to share their knowledge and creations should be supported to promote open access to knowledge and foster creativity. Application of international intellectual property conventions should be based on the fair balance between the interests of the rights holders and of the public.
18. Member States are responsible for ensuring an inclusive, relevant, up-to-date and legal environment for the development of the information society.

9.1.3 Ethics Complaint Procedures: (ISC)² *Code Of Ethics .*

Preamble

(ISC)² members are professionals and are expected to behave in an ethical manner. They are expected to make difficult ethical decisions and to support one another in doing so. While the board recognizes its obligation to provide the certificate holder with guidance on making ethical decisions, it does not expect to supervise or judge professionals in making these difficult decisions. The board recognizes its responsibility to maintain the integrity of the certification. It accepts that, from time to time, the good of the profession may require it to disassociate the profession from egregious behavior on the part of a particular certificate holder. It intends to deal with necessary complaints in a timely manner.

This document describes the procedure to be used when complaints are necessary. By publishing these procedures, the board does not expect, invite, solicit, or encourage such complaints. The use of these procedures is for the sole purpose of protecting the reputation of the profession. They are not intended to be used to coerce or punish certificate holders.

Confidentiality

The board and its agents undertake to keep the identity of the complainant and respondent in any complaint confidential from the general public. While disclosure of the identity of the complainant will be avoided where possible, upon filing a complaint, the complainant implies consent to disclose his identity to the respondent, where the board or its agents deem it necessary for due process. Actions of the board may be published at its discretion. Parties are encouraged to maintain confidentiality and certificate holders are reminded of their obligation to protect the profession.

Specificity of Complaints

The committee will consider only complaints that specify the canon of our (ISC)² *Code Of Ethics* that has been violated. If you are unsure of the canon violated, file the complaint to the best of your ability or contact the Ethics Committee contact listed at the end of these procedures.

The Ethics Committee

The Ethics Committee is established by the Board of Directors to hear all ethics complaints and make recommendations to the board. The committee chairman is selected by the board chairman every year. The members of the committee serve at the convenience and

discretion of the committee chairman. The current committee members have been in place for several years and diligently served in their capacity. As complaints and responses are received, the committee reviews both sides and renders a recommendation to the board for a final decision.

Standing of Complainant

Complaints will be accepted only from those who claim to be injured by the alleged behavior. While any member of the public may complain about a breach of Canons I or II, only principals (those with an employer/contractor relationship with the certificate holder) may complain about violations of Canons III, and only other professionals (those who are certified or licensed as a professional AND also subscribe to a code of ethics) may complain about violations of Canon IV.

Form of Complaints

All complaints must be in writing. The committee is not an investigative body and does not have investigative resources. Only information submitted in writing will be considered. Two copies must be submitted. At least one in written form and the other either in PDF or written form.

Complaints must be in the form of sworn affidavits. The committee will not consider allegations in any other form.

Complaints should be sufficiently complete to enable the board to reach an appropriate judgment. At a minimum, the affidavit should specify the respondent, the behavior complained of, the canon breached, the standing of the complainant, and any corroborating evidence.

Neither the board nor its committee is an investigative body and neither has the authority to compel testimony. We can consider only evidence submitted to us voluntarily. There may be many cases where this evidence is not sufficient to support any action. We can proceed only where a prima facie case is made. Where no such case is made, the committee will close the complaint without prejudice to either party.

Committee Procedures

Where a prima facie case has been made, the Ethics Committee will review and tender a recommendation to the board.

Rights of Respondents

Respondents to complaints are entitled to timely notification of complaints. It is the intent of the board and its agents to notify the respondent within thirty days from receipt of the complaint. The respondent is entitled to see all complaints, evidence, and other documents. The respondent will have thirty days from accepting and acknowledging delivery to submit information in defense, explanation, rebuttal, extenuation, or mitigation. As with the complaint, in order to be considered this information must be in the form of a sworn affidavit. As in the law, silence implies consent. That is, to the extent that the respondent is silent, the committee may assume that he does not dispute the allegations. The committee may grant necessary extensions of time to the respondent upon request.

Disagreement on the Facts

Where there is disagreement between the parties over the facts alleged, the Ethics Committee, at its sole discretion, may invite additional corroboration, exculpation, rebuttals and sur-rebuttals in an attempt to resolve such dispute. The committee is not under any obligation to make a finding where the facts remain in dispute between the parties. Where the committee is not able to reach a conclusion on the facts, the benefit of all doubt goes to the respondent. That is to say, where the respondent disputes the facts alleged, then the burden of proof is on the complainant.

Findings and Recommendations

The Ethics Committee will submit findings and recommendations for action to the board. In reaching its findings, the committee will consider any published guidance that has been given to certificate holders. In reaching its recommendations, the committee will prefer the most limited and conservative action consistent with its findings.

Notification and Right of Comment

The Ethics Committee will notify the parties of its recommendation prior to any board action. Parties have 14 days submit a response or comments on the recommendations for consideration by the board.

Disciplinary Action

Discipline of certificate holders is at the sole discretion of the board. Decisions of the board are final.

Final Disposition

Parties will be notified of the final disposition within thirty days of board action.

9.1.4 Unified Framework of Professional Ethics for Security Professionals

Integrity

Perform duties in accordance with existing laws, exercising the highest moral principles.

* Refrain from activities that would constitute a conflict of interest
* Act in the best interests of stakeholders consistent with public interest
* Act honorably, justly, responsibly, and legally in every aspect of your profession.

Objectivity

Perform all duties in a fair manner and without prejudice

* Exercise independent professional judgment, in order to provide unbiased analysis and advice.

* When an opinion is provided, note it as opinion rather than fact.

Professional Competence and Due Care

Perform services diligently and with professionalism

* Act with diligence and promptness in rendering service.
* Render only those services for which you are fully competent and qualified.
* Ensure that work performed meets the highest professional standards. Where resource constraints exist, ensure that your work is both correct and complete within those limits. If, in your professional judgment, resources are inadequate to achieve an acceptable outcome, so inform clients and principals.
* Be supportive of colleagues, and encourage their professional development. Recognize and acknowledge the contributions of others, and respect the decisions of principals and co-workers.
* Keep stakeholders informed regarding the progress of your work.
* Refrain from conduct which would damage the reputation of the profession, or the practice of colleagues, clients, and employers.
* Report ethical violations to the appropriate governing body in a timely manner.
* Participate in learning throughout your career, to maintain the skills necessary to function effectively as a member of the profession.

Confidentiality

Respect and safeguard confidential information and exercise due care to prevent improper disclosure.

* Maintain appropriate confidentiality of proprietary and otherwise confidential information encountered in the course of professional activities, unless such action would conceal, or result in, the commission of a criminal act, is otherwise required by law, or is authorized by the principal.

9.2 List of relevant documents provided by the Article 29 Data Protection Working Party and the European Data Protection Supervisor and ENISA

9.2.1 Article 29 Data Protection Party: Opinions, Working Documents, Recommendations and Annual Reports

Opinion 04/2012 on Cookie Consent Exemption[91]
Opinion 03/2012 on developments in biometric technologies[92]
Opinion 02/2012 on facial recognition in online and mobile services[93]

[91] Available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp194_en.pdf
[92] Available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf
[93] Available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp192_en.pdf

Opinion 14/2011 on data protection issues related to the prevention of money laundering and terrorist financing[94]
Opinion 13/2011 on Geolocation services on smart mobile devices[95]
Working Document 01/2011 on the current EU personal data breach framework and recommendations for future policy developments[96]
Opinion 10/2011 on the proposal for a Directive of the European Parliament and of the Council on the use of passenger name record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime[97]
Opinion 9/2011 on the revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications[98]
13th Annual Report on the situation regarding the protection of individuals with regard to the processing of personal data in the European Union and in third countries covering the year 2009[99]

9.2.2 European Data Protection Supervisor, Recommendations on the proposed Directive

Eurodac Central Unit - Inspection Report, June 2012[100]

Regulation establishing the Visa Information System[101]. Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation), OJ L 218, 13.8.208, p. 60-81.

Security Audit - Summary Report[102]. On 7 June 2012, the EDPS delivered the report on the results of a security audit on the VIS system to the European Commission, the European Parliament, the Council and the national data protection authorities involved in the coordinated supervision of the system.

Annual Report on the activities of the European Data Protection Supervisor (EDPS) to the European Parliament, the Council and the European Commission, in accordance with

[94] Available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp186_en.pdf
[95] Available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp185_en.pdf
[96] Available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp184_en.pdf

[97] Available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp181_en.pdf
[98] Available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp180_en.pdf
[99] Available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/annual-report/files/13th_annual_report_en.pdf
[100] Available at: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Eurodac/12-06-14_EURODAC_inspection_report_EN.pdf
[101] Available at: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/VIS/08-07-09_Regulation_VIS_EN.pdf
[102] Available at: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/VIS/12-06-01_VIS_security_audit_report_summ_EN.pdf

Regulation (EC) No 45/2001 of the European Parliament and of the Council and Article 16 of the Treaty on the Functioning of the European Union, which has replaced Article 286 of the EC Treaty[103].

Annual Report on the activities of the European Data Protection Supervisor (EDPS) to the European Parliament, the Council and the European Commission, in accordance with Regulation (EC) No 45/2001 of the European Parliament and of the Council, and Article 16 of the Treaty on the Functioning of the European Union, which has now replaced Article 286 of the EC Treaty[104].

9.2.3 European Network and Information Security Agency (ENISA)

Cooperation between CERTs and Law Enforcement Agencies in the fight against cybercrime a first collection of practices[105]. The essential aim of this report is to improve the capability of CERTs, with a focus on the national/governmental CERTs (n/g CERTs), to address the network and information security (NIS) aspects of cybercrime. It focuses particularly on supporting n/g CERTs and their hosting organisations in the European Union (EU) Member States in their collaboration with the LEAs. It also intends to be a first collection of practices collected from mature CERTs in Europe, including among other things workflows and collaboration with other key players, in particular different law enforcement authorities, in the fight against cybercrime.

Study on data collection and storage in the EU[106]. Given the clear contrast between the importance of the privacy by design principle on the one hand, and the reality of lax data protection practices with many online service providers on the other hand, the aim of this study is to present an analysis of the relevant. Legal framework of European Member States on the principles of minimal disclosure and the minimum duration of the storage of personal data. The study is not intended to go too deep into the details of the legal complexities of the data protection legislation. It rather focuses on a limited number of relevant use cases and tries to find out how the aforementioned principles are expressed in concrete legal or regulatory provisions applicable to these cases, and how they are observed in practice.

WORK PROGRAMME 2012 Improving Information Security Through Collaboration[107]

Securing Europe's Information Society. ENISA General Report 2010[108]

[103] Available at: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Annualreport/2011/AR2011_EN.pdf

[104] Available at: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Annualreport/2010/AR2010_EN.pdf

[105] Available at: http://www.enisa.europa.eu/activities/cert/support/supporting-fight-against-cybercrime/cooperation-between-certs-and-law-enforcement-agencies-in-the-fight-against-cybercrime-a-first-collection-of-practices

[106] Available at: http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/data-collection

[107] Available at: http://www.enisa.europa.eu/publications/programmes-reports/WP2012.pdf

[108] Available at: http://www.enisa.europa.eu/publications/programmes-reports/TPAB11001ENC.pdf

9.2.4 Relevant preparatory Acts (related to the EU Protection of Personal Data reform)

- COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Safeguarding Privacy in a Connected World A European Data Protection Framework for the 21st Century[109]. Date of document: 25/01/2012
- COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS A comprehensive approach on personal data protection in the European Union[110]. Date of document: 04/11/2010
- REPORT FROM THE COMMISSION TO THE COUNCIL AND THE EUROPEAN PARLIAMENT Evaluation report on the Data Retention Directive (Directive 2006/24/EC)[111]. Date of document: 18/04/2011
- Opinion of the European Data Protection Supervisor on the proposal for a regulation of the European Parliament and of the Council concerning customs enforcement of intellectual property rights. Official Journal C 363, 13/12/2011 P. 0001 - 0005[112]. Date of publication: 13/12/2011
- Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL establishing for the period 2014 to 2020 the Rights and Citizenship Programme[113]. Date of document: 15/11/2011
- Recommendation for a Council Decision on the vote to be taken by Member States within the competent bodies of the Council of Europe, on behalf of the European Community, in favour of adopting the draft Recommendation on the protection of personal data collected and processed for insurance purposes, and of authorizing the publication of its Explanatory Memorandum[114]. Date of document: 18/03/2002
- Decision on the joint text approved by the Conciliation Committee for a European Parliament and Council Directive concerning the processing of personal data and the protection of privacy in the telecommunications sector (C4- 0571/97 00/0288(COD)) Official Journal C 371 , 08/12/1997 P. 0174[115]. Date of document: 20/11/1997
- Decision on the common position established by the Council with a view to the adoption of a European Parliament and Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement

[109] Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52012DC0009:EN:NOT

[110] Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52010DC0609:EN:NOT

[111] Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52011DC0225:EN:NOT

[112] Available at: http://eur-ex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52011XX1213%2801%29:EN:NOT

[113] Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52011PC0758:EN:NOT

[114] Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52002SC0280:EN:NOT

[115] Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:51997AP0361:EN:NOT

of such data (C4-0051/95 - 00/0287(COD)) (Codecision procedure: second reading)Official Journal C 166 , 03/07/1995 P. 0105[116].

- The Stockholm Programme — An open and secure Europe serving and protecting citizens. Official Journal C 115 , 04/05/2010 P. 0001 - 0038[117].
- COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Overview of information management in the area of freedom, security and justice[118]. Date of document: 20/07/2010
- COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT Accompanying document to the Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on attacks against information systems, and repealing Council Framework Decision 2005/222/JHA {COM(2010) 517 final} {SEC(2010) 1123 final}[119]
- Strengthening security and fundamental freedoms on the Internet European Parliament recommendation of 26 March 2009 to the Council on strengthening security and fundamental freedoms on the Internet (2008/2160(INI)) Official Journal C 117 E , 06/05/2010 P. 0206 - 0213[120]
- Opinion of the European Economic and Social Committee on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions — A comprehensive approach on personal data protection in the European Union COM(2010) 609 final.Official Journal C 248 , 25/08/2011 P. 0123 - 0129[121]
- Opinion of the European Data Protection Supervisor on the Communication from the Commission on the global approach to transfers of Passenger Name Record (PNR) data to third countries. Official Journal C 357 , 30/12/2010 P. 0007 - 0011[122]
- Opinion of the European Data Protection Supervisor on the proposal for a Council Decision on the conclusion of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for purposes of the Terrorist Finance Tracking Program (TFTP II). Official Journal C 355 , 29/12/2010 P. 0010 - 0015[123]
- Opinion of the European Data Protection Supervisor on the proposal for a regulation of the European Parliament and of the Council concerning customs enforcement of intellectual property rights. Official Journal C 363 , 13/12/2011 P. 0001 - 0005[124]

[116] Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:51995AP0120:EN:NOT

[117] Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52010XG0504%2801%29:EN:NOT

[118] Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52010DC0385:EN:NOT

[119] Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52010SC1122:EN:NOT

[120] Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52009IP0194:EN:NOT

[121] Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52011AE0999:EN:NOT

[122] Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52010XX1230%2802%29:EN:NOT

[123] Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52010XX1229%2802%29:EN:NOT

[124] Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52011XX1213%2801%29:EN:NOT

9.2.5 General Data Protection Regulation

On 25th of January 2012, the European Commission proposed a comprehensive reform of the EU's 1995 data protection rules to strengthen online privacy rights and boost Europe's digital economy.

The main topics within the Proposal for a Regulation of the European Parliament and the Council on the protection of individuals with regard to the processing or personal data on the free movement of such data (General Data Protection Regulation). COM(2012)11final. 2012/0011 (COD) are:

- **Legal Basis of the proposal:** This proposal is based on Article 16 TFEU, which is the new legal basis for the adoption of data protection rules introduced by the Lisbon Treaty. This provision allows the adoption of rules relating to the protection of individuals with regard to the processing of personal data by Member States when carrying out activities which fall within the scope of Union law. It also allows the adoption of rules relating to the free movement of personal data, including personal data processed by Member States or private parties. A Regulation is considered to be the most appropriate legal instrument to define the framework for the protection of personal data in the Union. The direct applicability of a Regulation in accordance with Article 288 TFEU will reduce legal fragmentation and provide greater legal certainty by introducing a harmonized set of core rules, improving the protection of fundamental rights of individuals and contributing to the functioning of the Internal Market.

- **Subsidiary and Proportionality:** According to the principle of subsidiary (Article 5(3) TEU), action at Union level shall be taken only if and in so far as the objectives envisaged cannot be achieved sufficiently by Member States, but can rather, by reason of the scale or effects of the proposed action, be better achieved by the Union. Member States cannot alone reduce the problems in the current situation, particularly those due to the fragmentation in national legislations. Thus, there is a specific need to establish a harmonized and coherent framework allowing for a smooth transfer of personal data across borders within the EU while ensuring effective protection for all individuals across the EU. The principle of proportionality requires that any intervention is targeted and does not go beyond what is necessary to achieve the objectives. This principle has guided the preparation of this proposal from the identification and evaluation of alternative policy options to the drafting of the legislative proposal.

- **Fundamental Rights Issues:** The right to protection of personal data is established by Article 8 of the Charter and Article 16 TFEU and in Article 8 of the ECHR. Data protection is closely linked to respect for private and family life protected by Article 7

of the Charter. This is reflected by Article 1(1) of Directive 95/46/EC which provides that Member States shall protect fundamental rights and freedoms of natural persons and in particular their right to privacy with respect of the processing of personal data. Other potentially affected fundamental rights enshrined in the Charter are the following: freedom of expression (Article 11 of the Charter); freedom to conduct a business (Article 16); the right to property and in particular the protection of intellectual property (Article 17(2)); the prohibition of any discrimination amongst others on grounds such as race, ethnic origin, genetic features, religion or belief, political opinion or any other opinion, disability or sexual orientation (Article 21); the rights of the child (Article 24); the right to a high level of human health care (Article 35); the right of access to documents (Article 42); the right to an effective remedy and a fair trial (Article 47).

9.2.6 EU Directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data

Framework Decision 2008/977/JHA has a limited scope of application, since it only applies to cross-border data processing and not to processing activities by the police and judiciary authorities at purely national level. This is liable to create difficulties for police and other competent authorities in the areas of judicial co-operation in criminal matters and police cooperation.

They are not always able to easily distinguish between purely domestic and cross border processing or to foresee whether certain personal data may become the object of a cross-border exchange at a later stage. The Framework Decision 2008/977/JHA does not contain any mechanism or advisory group similar to the Article 29 Working Party supporting common interpretation of its provisions, nor foresees any implementing powers for the Commission to ensure a common approach in its implementation.

A Directive is therefore the best instrument to ensure harmonization at EU level in this area while at the same time leaving the necessary flexibility to Member States when implementing the principles, the rules and their exemptions at national level. Given the complexity of the current national rules for the protection of personal data processed in the area of police cooperation and judicial co-operation in criminal matters, and the objective of comprehensive harmonization of these rules by way of this Directive, the Commission will need to request Member States to provide explanatory documents explaining the relationship between the components of the Directive and the corresponding parts of national transposition instruments in order to be able to carry out its task of overseeing the transposition of this Directive.

9.2.6.1 Legal Basis of the proposal

The proposal is based on Article 16(2) TFEU, which is a new, specific legal basis introduced by the Lisbon Treaty for the adoption of rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. The proposal aims to ensure a consistent and high level of data protection in this field, thereby enhancing mutual trust between police and judicial authorities of different Member States and facilitating the free flow of data and co-operation between police and judicial authorities.

9.2.6.2 Subsidiarity and Proportionality

The necessity of EU-level action in the areas of police and criminal justice on the following grounds:

- The right to the protection of personal data, enshrined in Article 8 of the Charter of Fundamental Rights and in Article 16(1) TFEU, requires the same level of data protection throughout the Union. It requires the same level of protection for data exchanged and data processed at domestic level.
- There is a growing need for law enforcement authorities in Member States to process and exchange at rapidly increasing rates for the purposes of preventing and combating transnational crime and terrorism. In this context, clear and consistent rules on data protection at EU level will help fostering co-operation between such authorities.
- In addition, there are practical challenges to enforcing data protection legislation and a need for co-operation between Member States and their authorities, which need to be organized at EU level to ensure unity of application of Union law. In certain situations, the EU is best placed to ensure effectively and consistently the same level of protection for individuals when their personal data are transferred to third countries.
- Member States cannot alone reduce the problems in the current situation, particularly those due to the fragmentation in national legislations. Thus, there is a specific need to establish a harmonized and coherent framework allowing for a smooth transfer of personal data across borders within the EU while ensuring effective protection for all individuals across the EU.

The principle of proportionality requires that any intervention is targeted and does not go beyond what is necessary to achieve the objectives. This principle has guided the

preparation of this proposal, from the identification and evaluation of alternative policy options to the drafting of the legislative proposal.

9.2.6.3 Fundamental rights issues

The right to protection of personal data is established by Article 8 of the Charter on Fundamental Rights of the EU and Article 16 TFEU as well in Article 8 of the ECHR. Data protection is closely linked to respect for private and family life protected by Article 7 of the Charter. This is reflected in Article 1(1) of Directive 95/46/EC, which provides that Member States shall protect fundamental rights and freedoms of natural persons and in particular their right to privacy with respect of the processing of personal data.

Other potentially affected fundamental rights enshrined in the Charter are the prohibition of any discrimination amongst others on grounds such as race, ethnic origin, genetic features, religion or belief, political opinion or any other opinion, disability or sexual orientation (Article 21); the rights of the child (Article 24) and the right to an effective remedy before a tribunal and a fair trial (Article 47).

9.2.6.4 Structure and Detailed explanation of the proposal

9.2.6.4.1 General provisions

Article 1 defines the subject matter of the Directive, i.e. rules relating to processing of

personal data for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal offences, and sets out the Directive's two-fold objective, i.e. to protect the fundamental rights and freedoms of natural persons and **in particular their right to the protection of personal data while guaranteeing a high level of public safety, and to ensure the exchange of personal data between competent authorities within the Union**.

Article 2 defines the scope of application of the Directive. **The scope of the Directive is not limited to cross-border data processing but applies to all processing activities carried out by 'competent authorities'** (as defined in Article 3(14)) for the purposes of the Directive. The Directive applies neither to processing in the course of an activity which falls outside the scope of Union law, nor to processing by Union institutions, bodies, offices and agencies, which is subject to **Regulation (EC) No 45/2001** and other specific legislation.

Article 3 contains definitions of terms used in the Directive. While some definitions are taken over from Directive 95/46/EC and Framework Decision 2008/977/JHA, others are modified, complemented with additional or newly introduced elements. **New definitions are those of 'personal data breach', 'genetic data' and 'biometric data', 'competent authorities'**

(based on Article 87 TFEU and Article 2(h) of Framework Decision 2008/977/JHA) and, of a 'child', based on the UN Convention on the Rights of the Child.

9.2.6.4.2 Principles

Article 4 sets out the principles relating to processing of personal data reflecting Article 6 of Directive 95/46/EC and Article 3 of Framework Decision 2008/977/JHA, while adjusting them to the particular context of this Directive.

These principles are: **(a) processed fairly and lawfully; (b) collected for specified and legitimate purposes and not further processed in a way incompatible with those purposes; (c) adequate, relevant, and not excessive in relation to the purposes for which they are processed; (d) accurate and, where necessary, kept up to date; (e) Kept in a form which permits identification of data subjects for no longer than it is necessary for the purposes for which the personal data are processed; (f) processed under the responsibility and liability of the controller.**

Article 5 requires the distinction, as far as possible; between personal data of different categories of data subjects. This is a new provision, included neither in Directive 95/46/EC nor in Framework Decision 2008/977/JHA, but which had been proposed by the Commission in its original proposal for the Framework Decision23. It is inspired by the Council of Europe's Recommendation No R (87)15. Similar rules already exist for Europol and Eurojust.

Article 6 on **different degrees of accuracy and reliability** reflects principle 3.2 of Council of Europe Recommendation No R (87)15. Similar rules, as also included in the Commission's proposal for the Framework Decision, exist for Europol.

Article 7 sets out the grounds for lawful processing, when necessary for the performance of a task carried out by a competent authority based on national law, to comply with a legal obligation to which the data controller is subject, in order to protect the vital interests of the data subject or another person or to prevent an immediate and serious threat to public security. The other grounds for lawful processing in Article 7 of Directive 95/46/EC are not appropriate for the processing in the area of police and criminal justice.

Article 8 sets out a general prohibition of processing special categories of personal data and the exceptions from this general rule, building on Article 8 of Directive 95/46/EC and adding genetic data, following ECtHR case law.

Article 9 establishes a prohibition of measures based solely on automated processing of personal data if not authorized by law providing appropriate safeguards, in line with Article 7 of Framework Decision 2008/977/JHA.

9.2.6.4.3 Rights of the data subject

Article 10 introduces the obligation for Member States to ensure easily accessible and understandable information, inspired in particular by principle 10 of the Madrid Resolution on international standards on the protection of personal data and privacy, and to oblige controllers to provide procedures and mechanisms for facilitating the exercise of the data subject's rights. This includes the requirement that the exercise of the rights shall be in principle free of charge.

Article 11 specifies the obligation for Member States to ensure the information towards the data subject. These obligations are building on Articles 10 and 11 of Directive 95/46/EC, without separate articles differentiating whether the information is collected from the data subject or not, and enlarging the information to be provided. It lays down exemptions from the obligation to inform, when such exemptions are proportionate and necessary in a democratic society for the exercise of the tasks of competent authorities (inspired by Article 13 of Directive 95/46/EC and Article 17 Framework Decision 2008/977/JHA).

Article 12 provides the obligation for Member States to ensure the data subject's right of access to their personal data. It follows Article 12(a) of Directive 95/46/EC, adding new elements for the information of the data subjects (on the storage period, their rights to rectification, erasure, or restriction and to lodge a complaint).

Article 13 provides that Member States may adopt legislative measures restricting the right of access if required by the specific nature of data processing in the areas of police and criminal justice, and on the information of the data subject on a restriction of access, following Article 17(2) and (3) of Framework Decision 2008/977/JHA.

Article 14 introduces the rule that in cases where direct access is restricted, the data subject must be informed on the possibility of indirect access via the supervisory authority, which should exercise the right on their behalf and must inform the data subject on the outcome of its verifications.

Article 15 on the right to rectification follows Article 12(b) of Directive 95/46/EC, and, as regards the obligations in case of a refusal, Article 18(1) of Framework Decision 2008/977/JHA.

Article 16 on the right to erasure follows Article 12(b) of Directive 95/46, and, as regards the obligations in case of a refusal, Article 18(1) of Framework Decision 2008/977/JHA. It integrates also the right to have the processing marked in certain cases, replacing the ambiguous terminology "blocking", used by Article 12(b) of Directive 95/46/EC and Article 18(1) of Framework Decision 2008/977/JHA.

Article 17 on the rectification, erasure and restriction of processing in judicial proceedings provides clarification based on Article 4(4) of Framework Decision 2008/977/JHA.

9.2.6.4.4 Controller and Processor

General obligations

Article 18 describes the responsibility of the controller to comply with this Directive and to ensure compliance, including the adoption of policies and mechanisms for ensuring compliance.

Article 19 sets out that the Member States must ensure the compliance of the controller with the obligations arising from the principles of data protection by design and by default.

Article 20 on joint controllers clarifies the status of joint controllers as regards their internal relationship.

Article 21 clarifies the position and obligation of processors, following partly Article 17(2) of Directive 95/46/EC, and adding new elements, including that a processor that processes data beyond the controller's instructions is to be considered a co-controller.

Article 22 on processing under the authority of the controller and processor follows Article 16 of Directive 95/46/EC.

Article 23 introduces the obligation for controllers and processors to maintain documentation of all processing systems and procedures under their responsibility.

Article 24 concerns the keeping of records, in line with Article 10(1) of Framework Decision 2008/977, whilst providing further clarifications.

Article 25 clarifies the obligations of the controller and the processor regarding co-operation with the supervisory authority.

Article 26 concerns the cases where consultation with the supervisory authority is mandatory prior to the processing, based on Article 23 of Framework Decision 2008/977/JHA.

Data security

Article 27 on the security of processing is based on the current Article 17(1) of Directive 95/46 on the security of processing, and Article 22 of Framework Decision 2008/977/JHA, extending the related obligations to processors, irrespective of their contract with the controller.

Articles 28 and 29 introduce an obligation to notify personal data breaches, inspired by the personal data breach notification in Article 4(3) of the e-Privacy Directive 2002/58/EC, clarifying and separating the obligations to notify the supervisory authority (Article 28) and to communicate, in qualified circumstances, to the data subject (Article 29). Article 29 also provides for exemptions by referring to Article 11(4)

Data Protection Officer

Article 30 introduces an obligation for the controller to appoint a mandatory data protection officer who should fulfill the tasks listed in Article 32. Where several competent authorities are acting under the supervision of a central authority, functioning as controller, at least this central authority should designate such a data protection officer. Article 18(2) of Directive 95/46/EC provided the possibility for Member States to introduce such requirement as a surrogate to the general notification requirement of that Directive.

Article 31 sets out the standing of the data protection officer.

Article 32 provides the tasks of the data protection officer.

9.2.6.4.5 Transfer of Personal Data to Third Countries or International Organizations

Article 33 sets out the general principles for data transfers to third countries or international organizations in the area of police co-operation and judicial co-operation in criminal matters, including onward transfers. It clarifies that transfers to third countries may take place only if the transfer is necessary for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties..

Article 34 lays down that transfers to a third country may take place in relation to which the Commission has adopted an adequacy decision under Regulation …./../201X or specifically in the area of police co-operation and judicial co-operation in criminal matters, or, in the absence of such decisions, where appropriate safeguards are in place. As long as adequacy decisions do not exist, the Directive ensures that transfers can continue to take place on the basis of appropriate safeguards and derogations. It furthermore sets out the criteria for the Commission's assessment of an adequate or not adequate level of protection, and expressly includes the rule of law, judicial redress and independent supervision. The article also provides for the possibility for the Commission to assess the level of protection afforded by a territory or a processing sector within a third country. It introduces that a general adequacy decision adopted, following the procedures under Article 38 of the General Data Protection Regulation, shall be applicable within the scope of this Directive. Alternatively an adequacy decision can be adopted by the Commission exclusively for the purposes of this Directive.

Article 35 defines the appropriate safeguards needed prior to international transfers, in the absence of a Commission adequacy decision. These safeguards may be adduced by a legally binding instrument such as an international agreement. Alternatively, the data controller may on the basis of an assessment of the circumstances surrounding the transfer conclude that they exist.

Article 36 spells out the derogations for data transfer based on Article 26 of Directive 95/46/EC and Article 13 of Framework Decision 2008/977/JHA.

Article 37 obliges Member States to provide that the controller informs the recipient of any processing restrictions and takes all reasonable steps to ensure that these restrictions are met by recipients of the personal data in the third country or international organization.

Article 38 explicitly provides for international co-operation mechanisms for the protection of personal data between the Commission and the supervisory authorities of third countries, in particular those considered offering an adequate level of protection, taking into account the OECD's Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy of 12 June 2007.

9.2.6.4.6 National Supervisor Authorities

Independent Status

Article 39 obliges Member States to establish supervisory authorities, following Article 28(1) of Directive 95/46/EC and Article 25 Framework Decision 2008/977/JHA, enlarging the mission of these authorities to contribute to the consistent application of the Directive throughout the Union, which may be the supervisory authority established under the General Data Protection Regulation.

Article 40 clarifies the conditions for the independence of supervisory authorities, implementing case law of the Court of Justice of the EU29, inspired also by Article 44 of Regulation (EC) No 45/200130.

Article 41 provides general conditions for the members of the supervisory authority, implementing the relevant case law31, inspired also by Article 42(2)-(6) of Regulation (EC) 45/2001.

Article 42 sets out rules on the establishment of the supervisory authority, including on conditions for its members, to be provided by the Member States by law.

Article 43 on professional secrecy of the members and staff of the supervisory authority follows Article 28(7) of Directive 95/46/EC and Article 25(4) Framework Decision 2008/977/JHA.

Duties and Powers

Courts, when acting in their judicial authority, are exempted from the monitoring by the supervisory authority, but not from the application of the substantive rules on data protection.

Article 45 provides the obligation of Member States to provide for the duties of the supervisory authority, including hearing and investigating complaints and promoting the awareness of the public on risk, rules, safeguards and rights. A particular duty of the supervisory authorities in the context of this Directive is, where direct access is refused or

restricted, to exercise the right of access on behalf of data subjects and to check the lawfulness of the data processing.

Article 46 provides the powers of the supervisory authority, based on Article 28(3) of Directive 95/46/EC, Article 25(2) and (3) of Framework Decision 2008/977/JHA.

Article 47 obliges the supervisory authorities to draw up annual activity reports, based on Article 28(5) of Directive 95/46/EC. Directive 95/46/EC provided simply a general obligation to co-operate, without specifying further.

Cooperation

Article 48 introduces rules on mandatory mutual assistance whereas Article 28 (6)2 of Directive 95/46/EC provided simply a general obligation to co-operate, without specifying further

Article 49 provides that the European Data Protection Advisory Board, established by the General Data Protection Regulation, exercises its tasks also in relation to processing activities within the scope of this Directive. In order to provide complementary support, the Commission will seek the advice of representatives of authorities competent for the prevention, investigation, detection and prosecution of criminal penalties of the Member States, as well as representatives of Europol and Eurojust, by means of an expert group on the law-enforcement related aspects of data protection.

Remedies, Liability and Sanctions

Article 50 provides the right of any data subject to lodge a complaint with a supervisory authority, based on Article 28(4) of Directive 95/46/EC, and relates to any infringement of the Directive in relation to the complainant. It also specifies the bodies, organizations or associations which may lodge a complaint on behalf of the data subject and also in case of a personal data breach independently of a data subject's complaint.

Article 51 concerns the right to a judicial remedy against a supervisory authority. It builds on the general provision of Article 28(3) of Directive 95/46/EC and provides specifically that the data subject may launch a court action for obliging the supervisory authority to act on a complaint.

Article 52 concerns the right to a judicial remedy against a controller or processor, based on Article 22 of Directive 95/46/EC and Article 20 of Framework Decision 2008/977/JHA.

Article 53 introduces common rules for court proceedings, including the rights of bodies, organizations or associations to represent data subjects before the courts, and the right of supervisory authorities to engage in legal proceedings. The obligation of Member States to

ensure rapid court actions is inspired by Article 18(1) of the e-Commerce Directive 2000/31/EC32.

Article 54 obliges Member States to provide for the right to compensation. It builds on Article 23 of Directive 95/46/EC and Article 19(1) of Framework Decision 2008/977/JHA, extends this right on damages caused by processors and clarifies the liability of co-controllers and coprocessors.

Article 55 obliges Member States to lay down rules on penalties, to sanction infringements of the Directive, and to ensure their implementation.

Delegated Acts and Implementing Acts

Article 56 contains standard provisions for the exercise of delegations in line with Article 290 TFEU. This allows the legislator to delegate to the Commission the power to adopt no legislative acts of general application to supplement or amend certain non-essential elements of a legislative act (quasi-legislative acts).

Article 57 contains the provision for the Committee procedure needed for conferring implementing powers on the Commission in cases where, in accordance with Article 291TFEU, uniform conditions for implementing legally binding acts of the Union are needed. The examination procedure applies.

Final Provisions

Article 58 repeals Framework Decision 2008/977/JHA.

Article 59 sets out that specific provisions with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties in Union acts, regulating the processing of personal data or the access to information systems within the scope of the Directive, and adopted prior to the adoption of this Directive, remain unaffected.

Article 60 clarifies the relationship of this Directive with previously concluded international agreements by Member States in the field of judicial co-operation in criminal matters and police co-operation.

Article 61 provides for the obligation of the Commission to evaluate and report on the implementation of the Directive, in order to assess the need to align the previously adopted specific provisions referred to in Article 59 with this Directive.

Article 62 sets out the obligation of the Member States to transpose the Directive in their national law and notify to the Commission the provisions adopted pursuant to the Directive

Article 63 determines the date of the entry into force of the Directive.

Article 64 lays down the addressees of this Directive.

Some institutions have already adopted reports on both new instruments. Although the entry in force is not even determined, and some provisions can be modified on future versions, we want now to summarise the discussion. We start with an Opinion of Article 29 Data Protection Working Group, and then we will see the European Data Protection Supervisor Report on the 2012 Reform package.

9.3 Opinions from ARTICLE 29 DATA PROTECTION WORKING PARTY with regard to the two legislative proposals

9.3.1 Introduction: the 2012 Reform Package will improve current data protection guarantees?

The Working Party notes that the current proposal would result in lowering the data protection standards in several Member States. Obviously, it finds this to be unacceptable and therefore calls on the European legislator to ensure that the current, higher data protection safeguards in the European Union are to be considered as the bare minimum for the proposed Directive. Of course, it concedes that providing limitations and exceptions is necessary in the security field, notably concerning the rights of data subjects, but it must be made clear that these are exceptions and that the 'core' aspects are the same.

The Working Party notes and welcomes that the Directive has given up the distinction between the processing of personal data in domestic and in cross-border cases that was provided for under Framework Decision 2008/977/JHA. This limitation of the applicability of European legislation to strict cross-border cases has in the past been criticized by the Working Party.

The Working Party invites the European legislator to ensure no doubt can exist that the Directive applies to criminal procedures and the prosecution of crimes, also to avoid situations that no data protection would be offered as soon as a prosecutor or investigative judge is involved in a law enforcement operation or investigation, in line with Council of Europe Convention 108. The Working Party feels Article 44(2) needs clarification on the meaning and intention of the wording "to act in a judicial capacity". It should be clear what the relation between the DPA and the courts should be and under what circumstances supervisory tasks can be carried out.

9.3.2 Data processing principles

The Directive fails to include important elements regarding the retention of personal data (including retention periods), transparency towards individuals, keeping personal data up to date, and ensuring it is adequate, relevant and not excessive. Accountability provisions requiring the data controller to demonstrate compliance are also missing.

The Working Party suggests including provisions limiting access to data to duly authorized staff in competent authorities who need them for the performance of their tasks.

Regarding a lack of consistency with the Regulation, the Working Party welcomes the distinction that is proposed to several categories of data subjects to be processed. It notes in particular a distinction that is to be made between data regarding suspects, victims, witnesses, etc.

The Working Party recommends the distinction that has to be made based on the quality and accuracy of the data processed by the law enforcement authorities. The Working Party however regrets that these distinctions have been limited by adding the words “as far as possible” in Articles 5 and 6, and proposes to delete this wording. Also, it is concerned by the large scope of the so-called ‘miscellaneous category of data subjects’ (Article 5(1)(e)) about whom data can be processed. The Working Party suggests reformulating this category to ensure data about non-suspects can only be processed for a very limited amount of time and under strict conditions. The Directive should make clear that stricter rules on time limits and review have to apply to those groups of data subjects referred to under Article 5(1)(b-e).

Specific provisions should be introduced relating to the processing of personal data of children, as provided for by the Regulation. In particular, Member States should be compelled to provide age thresholds under which data should not be processed for the purposes of prevention, investigation, detection or prosecution of criminal offences without due justification, in particular if special categories of data are to be collected. Shorter storage periods in police and justice files should be provided by Member States for data concerning children.

The provision on special categories (Article 8) is slightly wider than in the framework Decision (2008/977/JHA). In addition, despite the inclusion of genetic data, there is no separate recital or an article on the handling of this kind of data. Such provision would however mean an important safeguard in relation to the use of genetic data and its retention periods.

Based on the derogation in Article 8(2) there is a real danger of allowing different levels of protection of personal data of special categories (sensitive data) under the Directive. The Working Party therefore suggests the European legislator amends this article to provide for harmonized implementation by further defining the required appropriate safeguards. In addition, the Working Party advises to include in paragraph 2 that the exceptions can only be used when in compliance with the conditions set out in Article 4.

9.3.3 Data subjects rights

The Directive should therefore make clear that any limitation to the data subjects’ rights can only be justified on a case-by-case basis, taking due account of the circumstances of the specific case and that each of these restrictions (and not only omission) has to be fully documented. The Working Party furthermore believes that a limitation to the right of access and information should also mean, that in certain cases, data subjects can still be partially informed of the processing of their data.

With regard to restrictions on rights, there is a need to stipulate that the controller should assess on a case-by-case basis whether the restriction to the rights should apply, and that any restriction must be in compliance with the Charter of Fundamental Rights of the European Union and with the Convention for the Protection of Human Rights and Freedoms, and in line with the case law of the European Court of Justice and the European Court of Human Rights, and in particular respect the essence of these rights and freedoms. The Working Party recommends including this wording in Article 13.

The Directive seems to be consistent with the Regulation relating to the right to rectification, the right to lodge a complaint, the right to a judicial remedy against the national DPA, data controller and data processor, and the right to compensation and liability.

However, the Directive does not provide any right to object to the processing of personal data. There are many situations where data subjects, victims or witnesses should be able to have their data marked to limit further processing at the end of legal proceedings.

The way the rights of individuals can be exercised needs to be aligned more with the procedures described in the Regulation.

9.3.4 Data controller obligations

Under the Directive the data controller is not obliged to inform the individual if they intend to transfer personal data to a third country, and it is not clear why this has been excluded, particularly given member states are able to restrict the rights of individuals in certain circumstances.

The wording of the Directive is not consistent with the Regulation as regards data protection by design and by default and the Working Party sees no reason for this inconsistency. it urges to insert in the Directive provisions requiring a data protection impact assessment (DPIAs), including during the legislative procedure. It believes these are particularly important in the field of law enforcement processing of personal data, given the increased risks to individuals of this processing. The obligations relating to documentation also contain less detail than in the Regulation. The competent authorities covered by the Directive should at least also need to keep details of their DPO and retention periods.

The demands regarding the security of data are not very detailed and thus rather low compared to the current standards.

Provisions on breach notification should also be consistent across both instruments; however, the Working Party recognizes the differences in the law enforcement sector as regards notifying individuals.

The provisions on profiling and automated processing (Article 9) are inconsistent with the Regulation in that the Directive wording does not include relevant elements such as evaluating behavior.

9.3.5 International Transfers

General Principles for transfers and onward transfers: (1) The Working Party considers there is a need to make a clear distinction between onward transfers to third countries and international organization of personal data, allowing for additional restrictions for onward transfers, for example, taking into account a clear link to the purpose for which the data were originally collected and the prior consent of the sending authority: (2) the recipient of the data needs to be a competent authority in the meaning of the Directive.

Negative adequacy decisions: (1) The European legislator is therefore requested to adapt the provisions in such a way that it would be clear what the consequences of a so-called non-adequacy decision would be and how they would work in practice.

Transfers by way of appropriate safeguards: (1) With regard to Article 35, The Working Party considers that if such transfers are made on the basis of a self assessment, the competent authority needs to ensure the appropriate safeguards are laid down in a legally binding instrument; (2) the Working Party considers that the elements set out in Article 26(2) of Directive 95/46/EC need to be included, which as a minimum should be taken into account when making the self-assessment.

Derogations: (1) any derogation must be interpreted restrictively so that transfers done on this basis are the exception rather than the norm. It should also be avoided that the wording of the provisions could mean that a mere statement that the specific transfer is to be deemed necessary without further explanation would suffice to invoke these derogations and thus provide for extensive international transfers on a case-by-case basis without there being any safeguards in place for the protection of the personal data of the individual concerned.

The Working Party therefore considers that the wording of Article 36(c), (d) and (e) should narrow down the possibility of international transfers in individual cases. We therefore propose to include such an obligation by adding: "*2. The use of these derogations must be documented and the documentation must be made available to the supervisory authority on request*"; (2) the Working Party considers that Member States should have the possibility to decide whether and to what extent DPAs are involved in international transfers.

9.3.6 Powers of DPAs and co-operation

The Directive does not include provisions relating to access to premises as is provided for under the Regulation. The ability for the regulator to access the premises of the data controller when necessary should apply to all sectors.

The Directive provides for mutual assistance between DPAs, however, it does not contain the timescales prescribed in the Regulation. These risks a lack of consistency and the advice given relating to the timescales under the Regulation should be taken into account for both instruments. Equally, to ensure consistency across the two instruments, the Directive should include the possibility for DPAs to participate in joint operations.

9.3.7 Lack of critical issues

1. The Working Party regrets that the Directive does not contain provisions on the establishment of time limits, review and other safeguards as the limitation of use of data for

serious crimes etc. The Working Party takes note of Article 37 which provides for an obligation by the controller to inform the recipient of any processing restrictions and to take all reasonable steps to ensure they are met. However, Article 37 only applies to transfers to third countries. No justification is provided why the Directive does not include a similar rule when personal data is transferred between Member States of the Union. In such cases, the receiving Member States should also be obliged to respect any limitation of processing imposed by the transferring Member State. The Working Party is surprised that the Directive, in this respect, is a backwards step as compared to the Framework Decision 2008/977/JHA.

2. The Working Party notes that there is no obligation for the competent authorities that have transmitted data to inform the recipient that the transmitted data were incorrect or unlawfully transmitted. Such an obligation is crucial in an area of free flow of law enforcement information. Article 39(2) contains the possibility for Member States to decide that the DPA responsible for supervising the Regulation and the Directive may be the same. Taking due account of the national situations, especially in countries with sub-national DPAs, the Working Party would prefer if indeed a single DPA would be responsible for supervising both instruments. This would ensure consistency in the application of the rules.

3. The Working Party finally regrets that the Directive does not contain a provision on the transfer to private parties or other authorities, which are not a competent authority under the Directive. The Working Party therefore urges the European legislator to introduce a provision, allowing for transfers of law enforcement data to private parties only in narrowly defined circumstances defined by law.

9.4 Recommendations on the proposed Directive from the European Data Protection Supervisor

9.4.1 Horizontal issues (part III.2)

- Article 59: specific acts in the area of police and judicial cooperation in criminal matters should be amended at the latest at the moment the Directive enters into force.
- Add a new provision introducing an evaluation mechanism for regular evidence based assessments of whether data processing activities of a certain scale do actually constitute a necessary and proportionate measure for the purposes of preventing, detecting, investigation and prosecuting criminal offences.
- Add a new provision to ensure that transfer of personal data from law enforcement authorities to other public bodies or to private parties is only permissible under specific and strict conditions.
- Add a new provision on specific safeguards in relation to the processing of data of children.

9.4.2 Chapter I and II – General provisions and principles (part III.3 and III.4)

- Article 3(4): substantiate further in line with Article 17(5) of the proposed Regulation.
- Article 4(b): include clarification in a recital stating that the notion of 'compatible use' is to be interpreted restrictively.
- Article 4(f): align with Article 5(f) of the proposed Regulation and amend Articles 18 and 23 accordingly.

- Article 5: include non-suspected persons as a separate category. Delete 'as far as possible' and specify the consequences of the categorization.
- Article 6: delete 'as far as possible' in paragraphs 1 and 2.
- Article 7(a): change into a self standing provision ensuring in a general manner that all data processing operations are provided for by law, thereby fulfilling the requirements of the EU Charter of Fundamental Rights and ECHR.
- Article 7(b) to (d): replace by an additional, separate provision which exhaustively lists the grounds of public interest for which derogation to the purpose limitation principle can be allowed.
- Add a new provision on the processing of personal data for historical, statistical and scientific purposes.
- Add an obligation for the competent authority to put mechanisms in place to ensure that time limits are established for the erasure of personal data and for a periodic review of the need for the storage of the data, including fixing storage periods for the different categories of personal data as well as regular checks on their quality.
- Article 8: include the strict wording of recital 26 in Article 8. Include what is envisaged by suitable measures going beyond regular safeguards.

9.4.3 Chapter III – Rights of the data subject (part III.5)

- Article 10: delete the reference to 'all reasonable steps' in Article 10(1) and (2). Include an explicit time limit in Article 10(4) and state that information should be given to the data subject at the latest within one month of receipt of the request. Replace the wording 'vexatious' in Article 10(5) by 'manifestly excessive' and provide further guidance on this notion in a recital.
- Add a new provision requiring the controller to communicate to each recipient to whom the data have been disclosed, any rectification, erasure or change of the data either or not carried out in accordance with Article 15 or 16, unless this proves impossible or involves a disproportionate effort.
- Articles 11 and 13: add a sentence in Article 11(4) and Article 13(1) stating that the controller should be required to assess in each specific case by way of a concrete and individual examination whether partial or complete restrictions for one of the grounds applies. Ensure a limited interpretation of the scope of Article 11(5) and Article 13(2). Delete the word 'omitting' in Article 11(4) and Recital 33.
- Article 15 and 16: add grounds and conditions for restricting the right to rectification and the right to erasure.
- Article 16: use the wording 'shall restrict processing' instead of 'shall mark' in Article 16(3). Include in Article 16 the obligation for the controller to inform the data subject before lifting any restriction on processing.

9.4.4 Chapter V – Controller and processor (part III.6)

- Article 18: state, also in Article 4(f), that the documentation requirement stems from the general obligation to be able to demonstrate compliance with the Directive. Include a requirement to keep information on the legal ground on which the data is transferred, with a substantive explanation especially if a transfer is based on Article 35 or 36.
- Article 19: substantiate the notion of data protection 'by default'.
- Article 23(2): align with Article 28(2) of the proposed Regulation.
- Article 24: include the identity of the recipients of the data.

- Insert a new provision, requiring the competent authorities to carry out a DPIA, unless a specific assessment, equal to a DPIA, has already been made during the legislative process.
- Article 26: align more closely with the procedures developed in Article 34(2) of the proposed Regulation.
- Article 30: deal with the issue of conflict of interest and lay down a minimum term of office of two years.
- Article 31: provide for an appropriate administrative attachment with due regard for the independent role of the DPO and with a view in particular to avoiding possible uneven relations or influence by high rank controllers.

9.4.5 Chapter V – Transfer to third countries (part III.7)

- Article 33: add the requirement that the transfer may only take place if the controller in the third country or the international organization is a competent authority within the meaning of the proposed Directive.
- Article 35: delete Article 35(1)(b) or as a minimum include the requirement of a prior authorization of the supervisory authority.
- Article 36: clarify in a recital that any derogation used to justify a transfer needs to be Interpreted restrictively and should not allow the frequent, massive and structural transfer of personal data; even an individual case should not allow wholesale transfers of data and should be limited to data strictly necessary. Add additional safeguards such as the obligation to specifically document the transfers.
- Articles 35 and 36: add that in case of a negative decision on adequacy, transfers should be based (i) on Article 35(1)(a) if there is a legally binding international agreement allowing for the transfer under specific conditions guaranteeing an adequate protection, or (ii) on the derogations of Article 36(a) or (c).

9.4.6 Chapter VI and VII – Oversight mechanism (part III.8)

- Article 44: provide more guidance in a recital on what is meant to be covered by 'judicial capacity'.
- Article 46: align the powers of the supervisory authorities vis-à-vis national police Authorities with the powers under the proposal for a Regulation. Align Article 46(a) with Article 53 of the proposed Regulation and change the wording 'such as' in Article 46(a) and (b) into 'including'.
- Article 47: include that the annual activities report of the supervisory authorities must be presented to the national parliament and made public.
- Article 48: include the provisions of Article 55(2) to (7) of the proposed Regulation in Article 48.

Consider the need for an enhanced cooperation mechanism also in the scope of application of the proposed Directive.