End-User Driven Demo for CBRNe

Data Protection and

Privacy Issues Report

Deliverable No.: D82-2

Issue: 1.0

Date: 30/04/2013

Contract No. 313077

Dissemination Level:

PU	Public	X
PP	Project Private, 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)	

The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under Grant Agreement no. 313077

Document Information and Approval status

Contract number:	313077		
Project acronym:	EDEN		
Project Co-ordinator:	BAE Systems		
Document Responsible Partner:	UPV/EHU		
Document Type:	Contractual Report		
Document number:	D82-2		
Document Title:	Data Protection and Privacy Issues Report		
Document ID:	EDEN-WP80-DEL-D82-2		
Classification:	Unclassified		
Contractual Date of Delivery:	30/04/2014	**Actual date of delivery**	30/04/2014
Filename:	EDEN-WP80-DEL-D82-2-final		
Status:	Released		
Approval status			
Document Manager	**Verification Authority:**		**Project approval**
UPV/EHU	**WP80 Leader**		**EMB**

Distribution List

Name	Company/Institution
	EDEN Consortium
	European Commission

Executive Summary

Data management, data protection, and privacy concerns are likely to be a huge issue in CBRNE major crisis situations. Under those exceptional circumstances, these data are likely to be collected without the data subjects' consent, in highly stressful conditions, in the absence of normal infrastructure, and in the midst of political and legal uncertainty. Moreover, it is perfectly possible to imagine a situation when the authorities responsible for the lives and health of an entire population might need to gain access to databases which are usually highly protected in order to mitigate the consequences of a CBRNE major crisis event.

The aim of this report is to explore the legal framework of data protection and privacy issues under these unusual circumstances. The report starts by analysing public attitudes towards data protection and privacy issues, so as to compare their desires and hopes with the values included in the legislation currently ruling. It then surveys four related areas of the EU legal framework:

- Data protection and privacy as a fundamental right in the charter of fundamental rights of the European Union.
- Directive 45/96/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
- Proposal for a regulation of the European parliament and of the council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (general data protection regulation)
- Protection of personal data and the protection of privacy in the communication sector. Directive 2002/58/EC of the European parliament and of the council of 12 July 2002 (directive on privacy and electronic communications), amended by directive 2006/24/EC and by directive 2009/136/EC

The report continues with a description of the main institutions involved in data protection and privacy issues in the EU arena:

- The Article 29 – Data Protection Working Party
- The European Data Protection Supervisor

The report ends with a review of other relevant legal sources as well as State internal regulations relating to a declaration of a "State of Emergency", and a set of four case studies outlining the law in Spain France, Italy and Poland.

Partners Involved in Document

No	Partner	Short name	Check if involved
1	BAE Systems	BAES	
2	EADS Astrium	AST	
3	FFI	FFI	
4	Tecnoalimenti	TCA	
5	SELEX ES	SES	
6	SAMU	SAMU	
7	Main School of Fire Service	SGSP	
8	CSSC	CSSC	
9	Astri Polska	APL	
10	Istituto Affari Internazionali	IAI	
11	CBRNE LTD	CBRNELTD	
12	UCL	UCL	
13	LDI	LDI2	
14	Fraunhofer	FhG EMI	
14	Fraunhofer	FhG INT	
14	Fraunhofer	FhG ICT	
15	VTT	VTT	
16	FRS	FRS	
17	Indra	IND	
18	INERIS	INR	
19	SICPA	SIC	
20	MDA	MDA	
21	PIAP	PIAP	
22	Hotzone	HZS	
23	ENEA	ENEA	
24	Nucletudes	NUC	
24	OMNIDATA S.A	OMN	
26	University of the Basque Country	UPV/EHU	X
27	University of Reading	UREAD	
28	Bruker UK	BRU	
29	LDIAMON	LDIAMON	
30	Microfluidic	MCG	
31	Robert Koch	RKI	
32	EU-VRI	EU-VRI	
33	Space Research Center	SRC	
34	AINIA	AINIA	
35	UCSC	UCSC	
36	CBRNE Centre	UMU	

CONTENTS

LIST OF ABBREVIATIONS

CBRN	Chemical Biological Radiological Nuclear
CBRNE	Chemical Biological Radiological Nuclear Explosive
CECIS	Common Emergency Communication and Information System
COSI	Council Standing Committee on Internal security
EC	European Commission
ECDC	European Centre for Disease prevention and Control
ECHR	European Convention on Human Rights
ERCC	Emergency Response Coordination Centre
EU	European Union
INSC	Instruments for Stability, Nuclear and Security Cooperation
MS	Member state
TFEU	Treaty on the Functioning of the European Union

1 INTRODUCTION

Data management, data protection, and privacy concerns are likely to be a huge issue in CBRNE major crisis situations. Under those exceptional circumstances, these data are likely to be collected without the data subjects' consent, in highly stressful conditions, in the absence of normal infrastructure, and in the midst of political and legal uncertainty. Moreover, it is perfectly possible to imagine a situation when the authorities responsible for the live and health of an entire population might need to gain access to databases which are usually highly protected in order to mitigate the consequences of a CBRNE major crisis event: think, for instance, a scenario including bioterrorist attacks or sabotages against nuclear resources. Would it not be possible to think that in such circumstances national or supranational authorities would be willing to obtain as much information as possible? Would it not be true that they would be looking forward to knowing about the legal limitations on their capabilities and the attitudes of the EU citizens towards these issues?

The aim of this report is to provide for a general answer to these questions. However, we will firstly analyze the public attitudes towards data protection and privacy issues, so as to compare their desires and hopes with the values included in the legislation currently ruling. On this purpose, we will expose the main results of the Special Eurobarometer 359, entitled Attitudes on Data Protection and Electronic Identity in the European Union[1], which includes a lot of information relevant to our research, and the public consultations conducted by the EU institutions on 2009, which lasted for more than two years and included a high level conference in May of that same year. Then, we will concentrate on the main focus of this report, which is the legal framework applicable to data issues in major crisis emergencies in the Council of Europe, the EU and the national arena. On this purpose, we will expose the currently existing legislation.

Nevertheless, it is necessary to point out that the redaction of the main body of this report had to address a number of dilemmas from different nature. The first had to do with the legislation to be reviewed. As our report will show, there is not a specific normative framework on data protection and privacy issues related to CBRNE major crisis situations. Moreover, it is necessary to highlight that the plans regarding these events, such as the EU action plan on chemical, biological, radiological and nuclear security included in the Communication from the Commission to the European Parliament and the Council of 24 June 2009 on Strengthening Chemical, Biological, Radiological and Nuclear Security in the European Union – an EU CBRN Action Plan[2] does not make any mention to data and privacy

[1] See: http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf

[2] Available at: http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/jl0030_en.htm

issues. Thus, they must be addressed on the basis of the more common framework on data as such. As commonly known, the EU legislation on this topic depends on the Directive 45/96/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[3], which was adopted with two objectives in mind: to protect the fundamental right to data protection and to guarantee the free flow of personal data between Member States.However, this Directive, approved in 1995, is becoming quite old fashioned nowadays and does not seem able to fit those aims adequately[4].

That is why the EU corresponding authorities, that is, the European Parliament and the Council have prepared a Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)[5]. This Proposal has not originated new binding legislation, even if it seems clear that it will do so in the short term, after its approval by the EU Parliament. Under these circumstances, we had to make a decision on whether to concentrate on the legal framework currently existing or to focus on the new one which should be about to be approved. As might be guessed, we finally opted for a mixed solution, dedicating a part of our attention to both of them.

After addressing all these topics, we will dedicate the last part of our report to expose some concrete cases of national legislation, the cases of the Spanish, French, Italian and Polish regulatory frameworks related to data protection and privacy issues in CBRNE major crisis situations. On that part, we will make an exposition on the concrete response to the legal dilemmas previously mentioned, so as it could be much easier to build an idea about what could happen in a real major CBRNE crisis situation. Finally, we will arrive into some conclusions that hopefully may serve as guidelines for further analysis on these issues.

[3] Official Journal L 281 , 23/11/1995 P. 0031 – 0050.

[4] In fact, the Proposal states that "*The current framework remains sound as far as its objectives and principles are concerned, but it has not prevented fragmentation in the way personal data protection is implemented across the Union, legal uncertainty and a widespread public perception that there are significant risks associated notably with online activity11. This is why it is time to build a stronger and more coherent data protection framework in the EU, backed by strong enforcement that will allow the digital economy to develop across the internal market, put individuals in control of their own data and reinforce legal and practical certainty for economic operators and public authorities*"

[5]Brussels, 25.1.2012.COM(2012) 11 final. 2012/0011 (COD). C7-0025/12

2 PUBLIC ATTITUDES TOWARDS DATA PROTECTION AND PRIVACY ISSUES

As merely mentioned in our introduction, the issue of the public attitudes towards data protection and privacy issues has been deeply explored in the last years. There are three main efforts that should expressly be mentioned in that sense: the *Special Eurobarometer 359, entitled Attitudes on Data Protection and Electronic Identity in the European Union*[6], published in 2010; the *Consultation on the legal framework for the fundamental right to the protection of personal data,* conducted from 9 July to 31 December 2009; and the *Consultation on the Commission's comprehensive approach on personal data protection in the European Union* conducted from 4 November 2010 to 15 January 2011.

The *Special Eurobarometer 359, entitled Attitudes on Data Protection and Electronic Identity in the European Union* is especially important as far as it gathers the information corresponding to the attitudes towards these issues from public in general. This huge survey was conducted by TNS Opinion & Social at the request of Directorate-General Justice, Information Society & Media and Joint Research Centre between end of November and mid-December 2010, comprising all the 27 Member States of the EU[7]. It comprised 26.574 face-to-face interviews with Europeans aged 15 and over. All interviews were conducted in people's homes and in the appropriate national languages. Its results were analyzed at three levels: the average for the 27 Member States, the national average, and when relevant, the differences according to the socio-demographic characteristics of the respondents.

The results of the survey provide us for some relevant conclusions. The general impression is that most of the respondents considered data protection and privacy rights as important issues and, in general (55%), authorities and institutions, including the European Commission and the Parliament, are trusted more than commercial companies. In fact, a 70% of the people interviewed were concerned that their personal data held by companies might be used for a different purpose than the originally mentioned. Nevertheless, the importance of the different data varies considerably. Three-quarters of the European interviewees considered as the most important and personal information (and thus, the most sensitive) the financial information, such as salary, bank details and credit record (75%); medical information such as patient records, health information (74%); and national identity number and / or card number or passport number (73%). It must be also mentioned that a surprising three-quarter of people interviewed agreed on the idea that disclosing personal information is an increasing part of modern life, while around six out of ten respondents said

[6] See: http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf

[7] Croatia was not part of the EU at that moment.

that they agreed that the government of their country of residence asked them for more and more personal information (64%). It seems, thus, that most of the European population would consider it acceptable to permit a general access to some of their data if conditions made it necessary for public health or even security reasons. Nevertheless, this does not really apply to all kind of data. Instead, it seems that there are several areas where information seems to be more sensitive.

It is especially interesting to highlight that a huge majority of the EU citizens consulted considered that genetic information such as DNA data should deserve a special protection, which should share the same level than the information corresponding to health, sex life, ethnic origin, religious beliefs, or political opinions, etc., while only 7% say it should not. A country-by-country analysis shows that vast majorities in every single Member States agree that DNA data should have special protection. These majorities are largest in Slovakia (96%), Greece (95%), and Cyprus and Slovenia (94%) and smallest in Romania (80%) and Lithuania (78%). Lithuania also has one of the highest proportions of people who disagree (10%), along with Finland, Italy, Lithuania, Luxembourg and Sweden (all 10%), and to an even greater extent Belgium and Denmark (both 13%). However, those percent do not pass a 15% in any country. It may be also important to remark that the ratio of acceptation of the special range of gene data raised significantly when the respondent pertained to highly educated population, managers and active internet users. Thus, it must be kept in mind while balancing the different rights involved in the security/privacy discussion that data related to genes are considered as especially relevant by the EU citizens as indeed the current EU legal framework considers them to be.

It is also necessary to underline that most of the interviewed showed a special concern about data referring to minors. The Eurobarometer states that *"strongly convinced as they are that genetic information should have the same special protection as other sensitive information, the Europeans surveyed are even more convinced that minors should be specially protected from the collection and disclosure of personal data (95%) and also that minors should be warned of the consequences of collecting and disclosing personal data (96%)"*[8]. This statement was in shared by all Member States. Italy, which was the country were the opposition to this special consideration showed the highest percent, it did not pass over a 10%. Therefore, a second important conclusion is that data protection should be significantly increased when minor might be involved.

A third very important factor to highlight is that most of the interviewed were reluctant to accept that the police could gain access to private data if it was not linked to a concrete investigation. Indeed, only a third of them considered that the police should be able

[8]Page 196.

to access personal data for all general crime prevention activities. Even if we could not guess what they would have answered had the survey included a major crisis situation in the questionnaire, the available information should make us conclude that most people would prefer not to be acceded to their personal information if this is not strictly necessary due to relevant reasons.

The results of the Eurobarometer were adequately complemented by the information gathered by the EU institutions thanks to the public consultations conducted in 2009-2010. According to their results, the values included in the EU main legislative bodies seemed to match with the stakeholders' opinions. In fact, 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[9] stated that *"the findings confirmed that the core principles of the Directive are still valid and that its technologically neutral character should be preserved".*

Thus, the general conclusion that might be addressed is that all stakeholders, policy makers and lay people agree on the fact that data protection and privacy are extremely important issues and individual right to intimacy should be guaranteed by legislation. Moreover, it is important to stress that there is also a common agreement on the idea that even in this case, rights corresponding to these values should not be considered as unlimited. Indeed, most of the population, the institutional representatives, stakeholders and private agents consulted share the opinion that they should be balanced with another rights, such as, for instance, security. That is why we consider that the current legal framework seems to adequate to the values and interest of the EU citizens, as far as it provides for a solid defense of privacy, but it also entails an adequate balance with another rights, as we will show in the next pages of this report.

[9]COM(2010) 609 final. 4.11.2010. Available at: http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf

3 THE EU LEGAL FRAMEWORK: DATA PROTECTION AND PRIVACY AS A FUNDAMENTAL RIGHT IN THE CHARTER OF FUNDAMENTAL RIGHTS OF THE EUROPEAN UNION.

As it is commonly known, the Charter of Fundamental Rights of the European Union[10] is one of the most important documents ever produced by the EU Institutions. Moreover, it became a legal binding tool since the Treaty of Lisbon (Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, 13 December 2007[11]) was approved in 2007[12]. The data protection and privacy issue is addressed in its article number 8:

Article 8. Protection of personal data

1. Everyone has the right to the protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

3. Compliance with these rules shall be subject to control by an independent authority.

According to this article, the EU established the right to the protection of personal data as a new fundamental right, distinct from the right to respect for private and family life, home and communications set out in Article 7 of the Charter. This was an important recognition of the importance of this issue, which had been already addressed at the time of the redaction of the Charter by the Directive 45/96/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.

Article 8 was based on several former legal tools. Firstly, it could be connected with Article 8 of the European Convention on Human Rights (ECHR), even if that document does not explicitly refer to data protection and privacy issues. Its linkage to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981), done

[10](2007/C 303/01).

[11] See: http://www.consilium.europa.eu/uedocs/cmsUpload/cg00014.en07.pdf

[12] Prior to that moment, its legal status was uncertain and its full legal effect was under discussion.

by the Council of Europe[13], is also remarkable. It is important to mention that its Preamble included an explicit reference to this issue: "*Considering that it is desirable to extend the safeguards for everyone's rights and fundamental freedoms, and in particular the right to the respect for privacy, taking account of the increasing flow across frontiers of personal data undergoing automatic processing"*. More important, its main body constituted as such a big step in the recognition of the right to privacy and data protection as a fundamental one. However, and as far as we will refer to it in the next paragraph we will not deepen in it at this moment.

Other key documents inspiring the Charter of Fundamental Rights are: the Convention on Human Rights and Biomedicine (1997), especially its Article 10 on 'Private life and right to information'; Article 17 of the International Covenant on Civil and Political Rights (ICCPR, 1966) and the General Comment No. 16 on Article 17 ICCPR (especially its paragraph 10 on personal data); Article 12 of the Universal Declaration of Human Rights (UDHR), and the Guidelines for the Regulation of Computerized Personal Data Files adopted by a resolution of the General Assembly of the United Nations on 14th December 1990; and the Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding Supervisory Authorities and Trans-border Dataflow (2001)[14].

The importance of the Charter is that it settles the principles which should guide the construction of both the EU and the Member States legal framework on data protection and privacy issues. Thus, it must be considered as the principal source of the right to privacy in the EU context and its content must be strictly followed by all legislation addressing this topic. Moreover, EU institutions must make sure that the EU citizen's right to gain access to their data and modify them is guaranteed. Currently, this obligation is being accomplished by the European Data Protection Supervisor, *"an independent supervisory authority devoted to* ***protecting personal data and privacy*** *and promoting good practice in the EU institutions and bodies"*[15].Furthermore, the Article 29 Data Protection Working Party was created in order to provide, for instance, expert opinions from Member State level to the Commission on questions of data protection[16].

In what refers to our research topic, that is, data protection and privacy in CBRNE major crisis situations, article 8.2 acquires and extraordinary relevance, as far as its final part

[13] Available at: http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm

[14] See: EU Network Of Independent Experts On Fundamental Rights, *Commentary of the Charter of Fundamental Rights of the European Union*, June 2006, p. 91. Available at: http://llet-131-198.uab.es/CATEDRA/images/experts/COMMENTARY%20OF%20THE%20CHARTER.pdf

[15] See: https://secure.edps.europa.eu/EDPSWEB/edps/EDPS?lang=en

[16] See: http://ec.europa.eu/justice/data-protection/article-29/index_en.htm

opens the gate to the possibility to obtain data from people without their explicit consent: "*data must be processed fairly for specified purposes and on the basis of the consent of the person concerned* ***or some other legitimate basis laid down by law****".* Keeping this part in mind, it seems obvious that the possibility to obtain personal data without the consent of the human being(s) involved has been recognized by the Charter, under some relevant conditions[17]. The most important is that the exception to the consent must have been included in a law. As we will show later on, it might perfectly happen that the restriction is not based on an EU law but a Member State one. This is not relevant in the sense of the Charter: the important matter is that this restriction is established by the applicable legislation and this legal framework describes in sufficient detail appropriate data protection conditions and requirements.

Therefore, we could arrive into an important conclusion: even if data protection and privacy are considered by the Charter as fundamental rights, this does not mean that they could not be limited when they clash with another relevant rights or goods, such as, for instance, public health, security, etc. As the Commentary of the Charter of Fundamental Rights of the European Union States, reacted by several experts on Human Rights, point out, *"while the EU institutions are under obligation to refuse totally or partly access to a document where disclosure would undermine the protection of personal data, this exception should not be interpreted so as not to disproportionately limit the right of access to documents. Hence, the crucial issue is to define the weight of the respective rights and to optimize the application of each of them, and even so that the right which loses in the process of weighing remain as far as possible relevant in the concrete case"*[18].

Thus, the problem relays on defining what are the concrete limitations that the statement included in article 8 about fairness (*data must be processed fairly)* promote. In our opinion, this issue could be redefined as how to conciliate the defense of privacy and the protection of data with the protection of another relevant values, such as, for instance, security. This is precisely the role to be assumed by legislation developing the Charter, which distinguishes between the different type of data and the circumstances that might let the authorities to gain access to them, circumstances which include, as might be guessed, major crisis situations.

[17] As the EU Network Of Independent Experts On Fundamental Rights state, *"The processing of personal data must also be adequate, relevant and not excessive in relation to the purposes for which they were collected and/or further processed. Finally, one of the requirements is that personal data must also be accurate and, where necessary, kept up to date. To guarantee the observance of all these requirements, individuals enjoy legally enforceable rights, notably the right to access and rectify personal data relating to them"* (EU Network Of Independent Experts On Fundamental Rights, *Commentary of the Charter of Fundamental Rights of the European Union*, o.c., p. 91-92).

[18] See: EU Network Of Independent Experts On Fundamental Rights, *Commentary of the Charter of Fundamental Rights of the European Union*, o. c., p. 92.

It is, thus, the time to refer to the concrete legal documents which address these issues in the EU context: the Directive 45/96/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 and the Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).

4 THE EU LEGAL FRAMEWORK: DIRECTIVE 45/96/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[19]

As previously stated, the main legal tool currently ruling on data protection and privacy issues in the UE scope is the Directive 45/96/EC of the European parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Directive 45/96/EC onwards). In our opinion, this directive was a laudable effort to encompass the changes that were happening at that time and some of its main statements may be perfectly applicable even nowadays. Its main principles, transparency of data collection, fair and lawful processing, purpose limitation and specification, data minimization, consent, right to access, object, correct and withdraw one´s data, etc., already remain as the values to be addressed by a legislation which wants to reach an adequate protection of privacy[20].

Nevertheless, it seems quite easy to sustain that lots of different technological developments have occurred since that moment till now. For instance, in 1995 it was hard to imagine the volume of transactions and data which internet might bring in the next years. That is why Directive 45796/EC needs to be updated. However, in the meantime, we must reflect that it is almost the only EU legislation referring to the issues this report is dedicated to and that is why we base our legal analysis on it, even if we know it will probably be substituted soon.

In order to underline the aspects of the Directive 45/96/EC which have a certain relevance in connection with CBRNE situations we have to analyse the exceptions established by the EU legislator to the general principles of personal data processing. On this respect, we will firstly refer to its Article 2, which sets some relevant definitions in order to allow an adequate interpretation of the text. Two of these definitions are particularly relevant to our research purposes:

(a) 'personal data' shall mean any information relating to an identified or identifiable

[19]Official Journal L 281 , 23/11/1995 P. 0031 – 0050.

[20]On this purpose, we will quote a BEUC, the European Consumers' Organization, report: "We fundamentally believe that the existing core principles of the Directive - fair and lawful processing, purpose limitation and specification, data minimization, consent, right to access, object, correct and withdraw one's data to name a few - remain relevant and must be retained. While the focus today is often related to data protection and privacy online, it is equally important to keep technology neutral principles. Moreover, many aspects of the Directive have not been explored to their full potential – let alone the poor level of compliance and enforcement. Indeed, we find it difficult to accept the arguments that the Directive does not fit to the online environment when the Directive is currently not complied with by various online players. Just because the future of the Directive is currently being discussed, it does not follow that it should no longer be complied with". See: BEUC, EU General Data Protection Framework, BEUC answer to the consultation, at:
http://ec.europa.eu/justice/news/consulting_public/0003/contributions/organisations/beuc_en.pdf

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;

(b) 'processing of personal data' ('processing') shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as 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;

The concept of "processing" as stated by article 2(b) Directive 45/96/EC is a very broad one when performed upon personal data and includes a multiplicity of operational acts such as collecting, recording, storage, alteration., etc. In fact, this interpretations has also been endorsed by the European Court of Justice (ECJ) in the Lindqvist case law, which stated that "The act of referring, on an internet page, to various persons and identifying them by name or by other means, for instance by giving their telephone number or information regarding their working conditions and hobbies, constitutes 'the processing of personal data wholly or partly by automatic means' within the meaning of Article 3(1) of 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"[21].

In order to set out some fundamental criteria for making data processing legitimate, articles 6 and 7 Directive 45/96/EC are clearly essentials in this field. According to HEREDERO HIGUERAS[22] the scientific literature imposes the performing of a double test previously to the processing of personal data. Firstly, the data have to satisfy the quality criteria set out by article 6 Directive 45/96/EC. In any case, the so referred data only can be processed if the previsions of article 7 and 8 Directive 45/96/EC are fulfilled.

Article 7 directive 45/96/EC establishes as a first rule in order to make data processing legitimate the unambiguous consent of the data subject. Nevertheless, and alternatively to this statement, personal data may also be processed, among others, when processing is necessary in order to protect the vital interests of the data subject[23], or when processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom data are

[21] ECJ Case C-101/01 of 6 November 2003

[22]See Manuel HEREDERO HIGUERAS, *La directiva comunitaria de protección de los datos de character personal*, Aranzadi Editorial, Pamplona, 1997, 110.

[23] Article 7(d) directive 45/96/EC

disclosed[24]. The two final statements could be particularly relevant in CBRNE situations as in most cases both vital interests of the data subject (article 7 (d) directive 45/96/EC) or performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (article 7 (e) directive 45/96/EC) do occur. According to Directive 45/96/EC personal data can be processed under such circumstances even when the data subject has no given his consent.

In any case, the conditions of article 7 directive 45/96/EC are not sufficient in order to the processing of special categories of data (like the ones revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and health or sex life) which, according to article 8.1 Directive 45/96/EC cannot be processed, unless one condition established in article 8.2 is fulfilled (one of the exceptions to the general rule set out in article 8.1 is the possibility of processing the referred special categories of data when the processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent –article 8.2.c Directive 45/96/EC–).Particular interest has to be afforded to the provisions of paragraphs 3 and 4,article 8 Directive 45/96/EC related to the processing of special categories of data.

At this point article 8.3 sets out that article 8.1 Directive 45/96/EC shall not apply where processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.

On top of that, article 8.4 Directive 45/96/EC states that subject to the provision of suitable safeguards, Member States may, for reasons of substantial public interest, lay down exemptions in addition to those laid down in paragraph 2 either by national law or by decision of the supervisory authority. CBRNE situations could be located in the previsions of article 8.4 Directive 45/96/EC allowing Member States on the basis of substantial public interests (public protection against disasters and emergency situations) to process even special categories of data (the ones revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership or concerning health or sex life) without the explicit consent of the data subject.

Recital 34 Directive 45/96/EC gives us an adequate criteria in order to make an interpretation of article 8.4 when it establishes that Member States must also be authorized, when justified by grounds of important public interest, to derogate from the prohibition on

[24] Article 7(e) directive 45/96/EC

processing sensitive categories of data where important reasons of public interest so justify in areas such as public health and social protection -especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system - scientific research and government statistics; whereas it is incumbent on them, however, to provide specific and suitable safeguards so as to protect the fundamental rights and the privacy of individuals.

Section VI Directive 45/96/EC refers to exemptions and restrictions and it is integrated by article 13 which states that Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in articles 6 paragraph 1 (need to respect the principle of quality of the data), article 10 (right to information in the case of direct collection of the data), article 11.1 (right to information in the case of indirect collection of the data), article 12 (data subject's right of access to data) and article 21 (publicizing of processing operations) when such restriction constitutes a necessary measure to safeguard, among others, (a) national security, (b) defense or (c) public security. CBRNE situations are typical ones when article 13 Directive 45/96/EC (exemptions and restrictions to some rights – access, information, etc.–)could apply on the basis of public or national security or defense reasons.

Recital 42, 43 and 44 Directive 45/96/EC are connected with the aforementioned provisions, explaining its real dimension. As stated in recital 42 Member States may, in the interest of the data subject or so as to protect the rights and freedoms of others, restrict rights of access and information. They may, for example, specify that access to medical data may be obtained only through a health professional.

According to recital 43 Directive 45/96/EC restrictions on the rights of access and information and on certain obligations of the controller may similarly be imposed by Member States in so far as they are necessary to safeguard, for example, national security, defense, public safety, or important economic or financial interests of a Member State or the Union, as well as criminal investigations and prosecutions and action in respect of breaches of ethics in the regulated professions. The list of exceptions and limitations should include the tasks of monitoring, inspection or regulation necessary in the three last-mentioned areas concerning public security, economic or financial interests and crime prevention. In any case, the listing of tasks in these three areas does not affect the legitimacy of exceptions or restrictions for reasons of State security or defense. Recital 44 states that Member States may also be led, by virtue of the provisions of Community law, to derogate from the provisions of this Directive concerning the right of access, the obligation to inform individuals, and the quality of data, in order to secure certain of the purposes referred to above.

Finally and referred to transfer of personal data to third countries, the general

principle is set in article 25 Directive 45/96 EC which states that the Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection. As exception to the previsions of article 25, article 26 establishes that by way of derogation from Article 25 and save where otherwise provided by domestic law governing particular cases, Member States shall provide that a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2) may take place on condition that:

(a) the data subject has given his consent unambiguously to the proposed transfer; or

(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken in response to the data subject's request; or

(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or

(d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defense of legal claims; or

(e) the transfer is necessary in order to protect the vital interests of the data subject; or

(f) the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.

Particular importance has to be given to article 26.1(d), as CBRNE situations can impose a transfer of personal data to a third country even when not ensuring an adequate level of protection, on the basis of important public grounds (fight against natural disasters, terrorist attacks, etc.).

5 THE EU LEGAL FRAMEWORK: PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA AND ON THE FREE MOVEMENT OF SUCH DATA (GENERAL DATA PROTECTION REGULATION)[25]

As merely mentioned, the changes produced since the approval of Directive 45796/EC made it necessary to substitute it for an updated version that, gathering the spirit and principles included in that Directive might face the current legal challenges related to data protection and privacy issues in a much better way. This was precisely the aim of the Proposal for a Regulation of the European Parliament and of the Council of the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), dated on 25 January of 2012.

As sometimes happens, the legislative process related to the final approval of this legal tool has taken quite a long time. However, it seems to be now in its final steps, as far as last 12 March 2014 the European Parliament gave its strong backing to the architecture and the fundamental principles of the Commission´s data protection form proposals, on both the General Data Protection Regulation and on the Data protection Directive in the law enforcement context. This means that the Parliament is now set in stone and will not change even if the composition of the Parliament changes following the European elections in May. Keeping this in mind, the Proposal is now in the next step of the ordinary legislative procedure, that is, the negotiation between the Parliament and the Council of the EU, which will take place in the next months. But, even if it might take some time and some changes will probably be adopted, it is quite easy to foresee that the Proposal will became a binding document in the next future. As a consequence, we will examine it in deep detail.

These aims have been addressed through two complementary legislative proposals: a proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation); and a proposal for a Directive of the European Parliament and of the Council 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.

Firstly we would like to point out that the Proposal includes three main innovations:

[25]Brussels, 25.1.2012.COM(2012) 11 final. 2012/0011(COD). C7-0025/12

1. One continent, one law: The Regulation will establish a single, pan-European law for data protection, replacing the current inconsistent patchwork of national laws. Thus, Companies operating in the EU territory will deal with one law, not 28.

2. One-stop-shop: The Regulation will establish a 'one-stop-shop' for businesses: companies will only have to deal with one single supervisory authority, not 28, making it simpler and cheaper for companies to do business in the EU.

3. The same rules for all companies – regardless of their establishment: Today European companies have to adhere to stricter standards than their competitors established outside the EU but also doing business on our Single Market. With the reform, companies based outside of Europe will have to apply the same rules. European regulators will be equipped with strong powers to enforce this: data protection authorities will be able to fine companies who do not comply with EU rules with up to 2% of their global annual turnover. European companies with strong procedures for protecting personal data will have a competitive advantage on a global scale at a time when the issue is becoming increasingly sensitive[26].

As might be guessed, these general objectives do not make any explicit reference to data protection and privacy rights issues. Indeed, it seems that the new regulation is much more focused on a different type of topics. However, it would be unfair to consider that the new legislation has introduced no changes in the former regulation. In fact, there are several previsions which address these issues. For instance, article 6 of the Proposal for a Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data states processing of personal data shall be lawful only if and to the extent that at least one of the following grounds applies:

(a) the data subject has given consent to the processing of their personal data for one or more specific purposes;

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

(d) processing is necessary in order to protect the vital interests of the data subject;

[26]See: EU Press release "Progress on EU data protection reform now irreversible following European Parliament vote", Strasbourg, 12 March 2014, available at: http://europa.eu/rapid/press-release_MEMO-14-186_en.htm

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(f) processing is necessary for the purposes of the legitimate interests pursued by a controller, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. This shall not apply to processing carried out by public authorities in the performance of their tasks.

Article 6 of the Proposal includes among the grounds that make lawful the processing of personal data the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

According to Recital 36 of the Proposal, where processing is carried out in compliance with a legal obligation to which the controller is subject or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of an official authority, the processing should have a legal basis in Union law, or in a Member State law which meets the requirements of the Charter of Fundamental Rights of the European Union for any limitation of the rights and freedoms. It is also for Union or national law to determine whether the controller performing a task carried out in the public interest or in the exercise of official authority should be a public administration or another natural or legal person governed by public law, or by private law such as a professional association. On the basis of the aforementioned statements CBRNE situations can give raise to the lawful processing of the personal data, even without the consent of the data subject.

Even when article 6 of the Proposal establishes a set of general principles for the processing of personal data, special categories of such personal data (like the ones revealing race or ethnic origin, political opinions, religion or beliefs, trade-union membership, genetic data or data concerning health or sex life or criminal convictions or related to security measures) is subjected to special conditions. Basically, the general principle set out by article 9 of the Proposal (Processing of special categories of personal data) is that the processing of the aforementioned personal data shall be prohibited. Exceptions are made for a limited number of cases (article 9.2 of the Proposal) one of which is the possibility of processing when it is necessary for the performance of a task carried out in the public interest, on the basis of the Union Law, or Member State Law which shall provide for suitable measures to safeguard the data subject's legitimate interests.

Recitals 41, 42 and 43 of the Proposal give an adequate explanation to the referred provisions which can be particularly helpful in order to connect them with a hypothetical case of CBRNE (and the consequent need of processing personal data).

At this point, personal data which are, by their nature, particularly sensitive and

vulnerable in relation to fundamental rights or privacy, deserve specific protection. Such data should not be processed, unless the data subject gives his explicit consent. However, derogations from this prohibition should be explicitly provided for in respect of specific needs, in particular where the processing is carried out in the course of legitimate activities by certain associations or foundations the purpose of which is to permit the exercise of fundamental freedoms.

Derogating from the prohibition on processing sensitive categories of data should also be allowed if done by a law, and subject to suitable safeguards, so as to protect personal data and other fundamental rights, where grounds of public interest so justify and in particular for health purposes, including public health and social protection and the management of health-care services, especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system, or for historical, statistical and scientific research purposes.

Moreover, the processing of personal data by official authorities for achieving aims, laid down in constitutional law or international public law, of officially recognized religious associations is carried out on grounds of public interest.

Following the criteria set out in Directive 45/96/EC the Proposal establishes in its Chapter III (Rights of the data subject), Section 5, article 21 (Restrictions) the possibility for the Union of a Member State to restrict by Law the scope of the obligations and rights provided in article 5 points (a) to (e) –need to respect the principle of quality of the data– and Articles 11 to 20[27] and Article 32[28], when such a restriction constitutes a necessary and proportionate measure in a democratic society to safeguard, among others, public security, the prevention, investigation, detection and prosecution of criminal offences or other public interests of the Union or of a Member State.

According to Recital 59 of the Proposal restrictions on specific principles and on the rights of information, access, rectification and erasure or on the right to data portability, the right to object, measures based on profiling, as well as on the communication of a personal data breach to a data subject and on certain related obligations of the controllers may be imposed by Union or Member State law, as far as necessary and proportionate in a democratic society to safeguard public security, including the protection of human life especially in response to natural or man-made disasters, the prevention, investigation and prosecution of criminal offences or of breaches of ethics for regulated professions, other public interests of the Union or of a Member State, in particular an important economic or

[27] Rights of the data subject, including Transparency and modalities (articles 11 to 13), Information and access to data (article 14 to 15) and Rectification and erasure (article 16 to 18) and Right to object and profiling (article 19).

[28] Communication of a personal data breach to the data subject.

financial interest of the Union or of a Member State, or the protection of the data subject or the rights and freedoms of others. Those restrictions should be in compliance with requirements set out by the Charter of Fundamental Rights of the European Union and by the European Convention for the Protection of Human Rights and Fundamental Freedoms.

Finally and related to the transfer of personal data to third countries or international organizations, CBRNE situations can give raise to exceptions to the general rule established in article 40 "any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organization may only take place if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organization to another third country or to another international organization". The requirements for such a transfer of personal data are set out in article 41 that underlines that a transfer may take place where the Commission has decided that the third country, or a territory or a processing sector within that third country, or the international organization in question ensures an adequate level of protection. Such transfer shall not require any further authorization"[29].

As an exception to these dispositions article 44 of the Proposal states that in the absence of an adequacy decision pursuant to Article 41 or of appropriate safeguards pursuant to Article 42, a transfer or a set of transfers of personal data to a third country or an international organization may take place only on condition that, among others, the transfer is necessary for important grounds of public interest.

The proposal of Regulation includes in its Chapter IX some provisions relating to specific data processing situations. At this level, article 81 of the Regulation related to the processing of personal data concerning health disposes that it must be on the basis of Union law or Member State law which shall provide for suitable and specific measures to safeguard the data subject's legitimate interests, and be necessary for, among others, reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety, inter alia for medicinal products or medical devices or other reasons of public interest in areas such as social protection, especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system.

The mentioned provisions have an enormous impact when considering the possibility of accessing to personal data in CBRNE situations.

[29] In addition to this statement article 42 of the Proposal refers to transfers by way of appropriate safeguards, and article 43 to transfers by way of binding corporate rules.

As stated by recitals 122 and 123 Proposal of Regulation the processing of personal data concerning health, as a special category of data which deserves higher protection, may often be justified by a number of legitimate reasons for the benefit of individuals and society as a whole, in particular in the context of ensuring continuity of cross-border healthcare. Therefore this Regulation should provide for harmonized conditions for the processing of personal data concerning health, subject to specific and suitable safeguards so as to protect the fundamental rights and the personal data of individuals. This includes the right for individuals to have access to their personal data concerning their health, for example the data in their medical records containing such information as diagnosis, examination results, assessments by treating physicians and any treatment or interventions provided. The processing of personal data concerning health may be necessary for reasons of public interest in the areas of public health, without consent of the data subject. In that context, "public health" should be interpreted as defined in Regulation (EC) No 1338/2008 of the European Parliament and of the Council of 16 December 2008 on Community statistics on public health and health and safety at work, meaning all elements related to health, namely health status, including morbidity and disability, the determinants having an effect on that health status, health care needs, resources allocated to health care, the provision of, and universal access to, health care as well as health care expenditure and financing, and the causes of mortality. Such processing of personal data concerning health for reasons of public interest should not result in personal data being processed for other purposes by third parties such as employers, insurance and banking companies.

6 THE EU LEGAL FRAMEWORK: PROTECTION OF PERSONAL DATA AND THE PROTECTION OF PRIVACY IN THE COMMUNICATION SECTOR. DIRECTIVE 2002/58/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL OF 12 JULY 2002 (DIRECTIVE ON PRIVACY AND ELECTRONIC COMMUNICATIONS) AMENDED BY DIRECTIVE 2006/24/EC AND BY DIRECTIVE 2009/136/EC

As previously mentioned, 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 requires Member States to ensure the rights and freedoms of natural persons with regard to the processing of personal data, and in particular their right to privacy. On the basis of this statement Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 (Directive on privacy and electronic communications) was adopted in 2002 and afterwards amended according to the necessities that new technological developments required. Thus, it is an important document in what refers to CBRNE major crisis situations, as far as it addresses issues as important as access to data in the communication sector. This is especially true in the case of the response phase, when an intervention on these data might be recommendable. Therefore, it is important to focus especially on the exceptions to the general principles that rule over data protection and privacy in the main body of the Directive.

In this sense, we will start focusing on article 15 (Application of certain provisions of Directive 95/46/EC), which establishes that Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5 (confidentiality of the communications), Article 6 (traffic data), Article 8(1), (2), (3) and (4) (presentation and restriction of calling and connected line identification), and Article 9 (location data other than traffic data) of this Directive. These articles includes restrictions to data protection and privacy rights when such restrictions constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defense, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorized use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC. To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) of the Treaty on European Union. Consequently it remains clear that CBRNE major crisis situations may allow important restrictions referred to the mentioned rights of the citizens involved in electronic communications.

According to this point recital 10 and 11 Directive 2002/58/EC in the electronic communications sector, Directive 95/46/EC applies in particular to all matters concerning protection of fundamental rights and freedoms, which are not specifically covered by the provisions of this Directive, including the obligations of the controller and the rights of individuals. Directive 95/46/EC applies to non-public communications services. Like Directive 95/46/EC, this Directive does not address issues of protection of fundamental rights and freedoms related to activities which are not governed by Community law. Therefore it does not alter the existing balance between the individual's right to privacy and the possibility for Member States to take the measures referred to in Article 15(1) of this Directive, necessary for the protection of public security, defense, State security (including the economic well-being of the State when the activities relate to State security matters) and the enforcement of criminal law. Consequently, this Directive does not affect the ability of Member States to carry out lawful interception of electronic communications, or take other measures, if necessary for any of these purposes and in accordance with the European Convention for the Protection of Human Rights and Fundamental Freedoms, as interpreted by the rulings of the European Court of Human Rights. Such measures must be appropriate, strictly proportionate to the intended purpose and necessary within a democratic society and should be subjected to adequate safeguards in accordance with the European Convention for the Protection of Human Rights and Fundamental Freedoms.

7 THE MAIN INSTITUTIONS INVOLVED IN DATA PROTECTION AND PRIVACY ISSUES IN THE EU ARENA: THE ARTICLE 29 – DATA PROTECTION WORKING PARTY AND THE EUROPEAN DATA PROTECTION SUPERVISOR.

7.1 The Article 29 – Data Protection Working Party

The Article 29 – Data Protection Working party was set up under the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995. In fact, it was article 29 which created the Party, but its statute was reflected both in articles 29 and 30. According to article 30, the Working Party has to fulfil four main tasks: (a) examine any question covering the application of the national measures adopted under this Directive in order to contribute to the uniform application of such measures; (b) give the Commission an opinion on the level of protection in the Community and in third countries; (c) advise the Commission on any proposed amendment of this Directive, on any additional or specific measures to safeguard the rights and freedoms of natural persons with regard to the processing of personal data and on any other proposed Community measures affecting such rights and freedoms; (d) give an opinion on codes of conduct drawn up at Community level.

Thus, it seems reasonable to conclude that Working Party should be considered as an influential body, which should address some of the most conflictive issues arising from data protection and privacy issues. In fact, in all the years passed since its creation, it has accomplished with its functions, providing us for a large number of options, working documents, recommendations, etc. We would like to highlight specially one of these documents, the Opinion of the need for a balanced approach in the fight against terrorism, adopted in 14 December 2001, which is especially relevant to the topic addressed by this report.

The Opinion states that the fight against terrorism has given rise to a reinforced measures of intrusion by public authorities into individuals' privacy and that new questionable measures are discussed or yet adopted 8 telephone tapping, prior and generalized retention of telecommunication data by electronic communications services providers and operators, adoption of measures enabling "real time" surveillance of citizens, surrender of the dual criminality principle as a condition for the exchange of certain personal data concerning criminals, sharing of personal data for different purposes as the fight against crime, immigration and Foreign Counterintelligence and premature transfer of personal data to third countries.

The Working Party underlines the necessity to take into account the long term impact of urgent policies rapidly implemented or envisaged at this moment. This long term

reflection is all the more necessary in view of the fact that terrorism is not a new phenomenon and cannot be qualified as a temporary phenomenon. The Working Party also underlines the obligation to respect the principle of proportionality in relation to any measure restricting the fundamental right to privacy as required by art. 8 of the European Convention on Human Rights and the relevant case-law. This implies inter alia, the obligation to demonstrate that any measure taken corresponds to a "imperative social need".

Furthermore, the Working Party recalls that the legislative measures limiting the right to privacy of individuals have to be accessible and foreseeable as regards their implications for the persons concerned. This is a requirement involving legislation sufficiently clear in its definitions of the circumstances, the scope and the modalities of the exercise of interference measures. The provisions have to be clear and go into detail to indicate under which circumstances the public authority is authorized to take measures limiting fundamental rights. They should in particular specify where such measures may be used and should exclude all general or exploratory surveillance and offer protection against arbitrary attacks from public authorities.

Therefore, as might be seen, this document is particularly relevant to CBRNE major crisis situations. In case they were created by a terrorist attack, it is clear that its existence will make it much easier to make decisions. Moreover, it is important to wonder if this opinion could not also be applicable to accidental CBRNE situations. From our point of view, most of it does, in fact, match with that aim, as far as major crisis situations response needs usually does not distinguish between the different causes that provoke them. Therefore, we will end these paragraphs outlining the importance that this opinion might have between facing such situations.

7.2 The European Data Protection Supervisor

The European Data Protection Supervisor was created by 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 such as data[30]. According to the regulations, the EDPS´ general objective is to ensure that the European institutions and bodies respect the right to privacy when they process personal data and develop new policies. This main aim is concreted in three different types of tasks to be accomplished by this body[31].

[30]Available at: http://ec.europa.eu/justice/policies/privacy/docs/application/286_en.pdf

[31]See: https://secure.edps.europa.eu/EDPSWEB/edps/EDPS?lang=en

Consultation: the EDPS advises the European Commission, the European Parliament and the Council on proposals for new legislation and a wide range of other issues having an impact on data protection. As part of this consultative role, the EDPS also intervenes in cases before the European Court of Justice that are relevant to his tasks.

Cooperation: the EDPS cooperates with other data protection authorities in order to promote consistent data protection throughout Europe. The central platform for cooperation with national data protection authorities is the Article 29 Working Party. In fact, both organisms have cooperated since the creation of the EDPS, especially in what concerns to the challenges involved in the new technological developments. EDPS also cooperates with EURODAC, European Dactyloscopy, which is the European central database for the comparison of fingerprints of asylum seekers, sharing responsibilities with national data protection authorities.

Supervision: It is, however, the supervision role which might be more interesting in terms of describing the role to be played by the EDPS monitors the processing of the personal data protection rules. In doing so, it cooperates with national data protection authorities, which have to notify the EDPS about processing operations involving sensitive personal data or likely to pose other specific risks. Thus, it seems quite clear that this institution should be involved in all measurements adopted that undermine the rights to data protection and privacy issues.

Peter Hustinx and Giovanni Buttarelli were appointed European Data Protection Supervisor (EDPS) AND Assistant Supervisor respectively by a joint decision of the European Parliament and the council. Assigned for a five-year term, they took office in January 2009. To our knowledge, and according to the official page of the European Data Protection Supervisor, they are still playing that role.

8 OTHER RELEVANT LEGAL SOURCES: THE REGULATION PRODUCED BY THE COUNCIL OF EUROPE

8.1 Introduction

The Council of Europe is not a part of the European Union architecture. In fact, it comprises a wider range of States than the EU and it is considered to be the continent's leading human rights organization[32]. However, insofar all Member States are also part of the Council of Europe, its conventions and resolutions are particularly important in the EU context.

In the concrete arena of data protection and privacy issues, the most remarkable legal tool produced by the Council of Europe are Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 1981 and the Convention for the protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine, usually called the Oviedo Convention, as far as it was signed in Oviedo (Spain) on 1997.

9.2.- The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 1981

The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 1981, usually called 108 Convention was drawn up within the Council of Europe by a committee of governmental experts under the authority of the European Committee on Legal Co-operation (CDCJ), and opened for signature by the Member States of the Council of Europe on 28 January 1981 in Strasbourg[33].

The main interest of this Convention relays on the fact that it was the first legally binding international instrument adopted in the field of data protection. Indeed, nowadays it still remains the only binding international legal instrument with a worldwide scope of application in the field of data privacy, open to signature to any country, including all those which are not Members of the Council of Europe.

As stated in its article 1, its purpose was *"to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ("data protection")". In doing so, the Convention sets out a*

[32] See: http://www.coe.int/aboutCoe/index.asp?page=quisommesnous&l=en

[33] See: EPIC. "Council of Europe Privacy Convention", at: http://epic.org/privacy/intl/coeconvention/

whole range of minimum standards aimed at protecting the individuals against abuses which may accompany the collection and processing of personal data[34]. However, this protection is not unrestricted. Indeed, the Convention includes an article, article number 9 which describes what would be the exceptions and restrictions to this common framework:

> *Article 9 – Exceptions and restrictions*
>
> *No exception to the provisions of Articles 5, 6 and 8 of this convention shall be allowed except within the limits defined in this article.*
>
> *Derogation from the provisions of Articles 5, 6 and 8 of this convention shall be allowed when such derogation is provided for by the law of the Party and constitutes a necessary measure in a democratic society in the interests of:*
>
> *a. protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences;*
>
> *b. protecting the data subject or the rights and freedoms of others.*
>
> *Restrictions on the exercise of the rights specified in Article 8, paragraphs b, c and d, may be provided by law with respect to automated personal data files used for statistics or for scientific research purposes when there is obviously no risk of an infringement of the privacy of the data subjects.*

Thus, this article 9 of the Convention (Exceptions and restrictions) is the most important part of the whole document in terms of CBRNE major crisis situations, as it seems to be perfectly applicable to them. According to this disposition no exception to the provisions

[34] In its chapter II the Convention establishes the basic principles for data protection:

- Article 5: quality of data, which includes:
  a) fair and lawful obtaining and processing.
  b) Storage for specified and legitimate purposes and not used in a way incompatible with those purposes.
  c) Personal data undergoing automatic processing shall be adequate, relevant and not excessive in relation to the purposes for which they are stored.
  d) Personal data undergoing automatic processing shall be accurate and, where necessary, kept up to date.
  e) Personal data undergoing automatic processing shall be preserved in a form which permits identification of the data subjects no longer than is required fot the purpose for which those data are stored.
- Special categories of data (article 6): Personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards. The same shall apply to personal data relating to criminal convictions.

Additional safeguards for the data subject (article 8): Any person shall be enabled:

a) to establish the existence of an automated personal data file, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file.

b) to obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him are stored in the automated data file as well as communication to him of such data in an intelligible form;

c) to obtain, as the case may be, rectification or erasure of such data if these have been processed contrary to the provisions of domestic law giving effect to the basic principles set out in Articles 5 and 6 of this convention;

d) to have a remedy if a request for confirmation or, as the case may be, communication, rectification or erasure as referred to in paragraphs b and c of this article is not complied with.

of articles 5, 6 and 8 of the Convention shall be allowed except within the limits defined in this article. Derogation from the provisions of Articles 5, 6 and 8 of this convention shall be allowed when such derogation is provided for by the law of the Party and constitutes a necessary measure in a democratic society in the interests of protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences, protecting the data subject or the rights and freedoms of others. Restrictions on the exercise of the rights specified in Article 8, paragraphs b, c and d, may be provided by law with respect to automated personal data files used for statistics or for scientific research purposes when there is obviously no risk of an infringement of the privacy of the data subjects.

In order to make an adequate interpretation of the mentioned article 9, the Explanatory Report gives us some important references[35]. At this point, it is stated that exceptions to the basic principles for data protection are limited to those which are necessary for the protection of fundamental values in a democratic society. The text of the second paragraph of this article has been modelled after that of the second paragraphs of Articles 6, 8, 10 and 11 of the European Human Rights Convention. It is clear from the decisions of the Commission and the Court of Human Rights relating to the concept of "necessary measures" that the criteria for this concept cannot be laid down for all countries and all times, but should be considered in the light of the given situation in each country.

Litteraa *in paragraph 2* (article 9 Convention) lists the major interests of the State which may require exceptions (State security, public safety, the monetary interests of the State or the suppression of criminal offences). The concepts are particularly relevant in a

[35]Its Explicatory Report includes the following notes on this article:

> *55. Exceptions to the basic principles for data protection are limited to those which are necessary for the protection of fundamental values in a democratic society. The text of the second paragraph of this article has been modelled after that of the second paragraphs of Articles 6, 8, 10 and 11 of the European Human Rights Convention. It is clear from the decisions of the Commission and the Court of Human Rights relating to the concept of "necessary measures" that the criteria for this concept cannot be laid down for all countries and all times, but should be considered in the light of the given situation in each country.*
>
> *56. Litteraa in paragraph 2 lists the major interests of the State which may require exceptions. These exceptions are very specific in order to avoid that, with regard to the general application of the convention, States would have an unduly wide leeway.*
>
> *States retain, under Article 16, the possibility to refuse application of the convention in individual cases for important reasons, which include those enumerated in Article 9.*
>
> *The notion of "State security" should be understood in the traditional sense of protecting national sovereignty against internal or external threats, including the protection of the international relations of the State.*
>
> *57. The term "monetary interests of the State" covers all the different means of financing a State's policies. Accordingly, the term refers in particular to tax collection requirements and exchange control. The term "suppression of criminal offences" in this littera includes the investigation as well as the prosecution of criminal offences.*
>
> *58. Littera b concerns major interests of private parties, such as those of the data subject himself (for example psychiatric information) or of third parties (for example freedom of the press, trade secrets, etc.).*
>
> *59. Paragraph 3 leaves the possibility of restricting the exercise of the data subjects' rights with regard to data processing operations which pose no risk. Examples are the use of data for statistical work, in so far as these data are presented in aggregate form and stripped of their identifiers. Similarly, and in conformity with a recommendation of the European Science Foundation, scientific research is included in this category.*

CBRNE situation. These exceptions are very specific in order to avoid that, with regard to the general application of the convention; States would have an unduly wide leeway. States retain, under Article 16, the possibility to refuse application of the convention in individual cases for important reasons, which include those enumerated in Article 9.The notion of "State security" should be understood in the traditional sense of protecting national sovereignty against internal or external threats, including the protection of the international relations of the State.

Thus, one may arrive to a unique conclusion: according to the Convention, data protection and privacy rights could (and probably should) be limited in circumstances when *protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences* makes it necessary. This clause is especially relevant in term of response against CBRNE major crisis situations, as far as this type of crisis usually involve a great challenge against the good explicitly included in article 9. Therefore, we could conclude that this Convention allows the signing parties to impose restrictions to data protection and privacy rights when further interest are at stake, even if subject to some substantive limits that should be kept in mind when facing these situations. If we keep in mind that this Convention has been signed and ratified by all EU Member States[36], we could figure out how important this document could be in case of addressing a CBRNE major crisis situation.

8.2 The Convention for the protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine

The Convention on Human Rights and Biomedicine is a basic instrument at a regional European level related to the protection of Human Rights at the light of the new developments in the field of Biomedicine. It was, in fact, one of the first legal binding documents providing for a legal protection of the right to data protection and privacy in the biomedicine context. In that sense, it must be highlighted that its article 5 states that an intervention may only be carried out after the person concerned has given free and informed consent to it, having this person to be given beforehand appropriate information as to the purpose and nature of the intervention as well as on its consequences and risks[37]. Moreover, its article number 6 settles specific protection for all those who are unable to consent in a

[36] See: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=108&CM=&DF=&CL=ENG

[37] The concrete text is: *An intervention in the health field may only be carried out after the person concerned has given free and informed consent to it. This person shall beforehand be given appropriate information as to the purpose and nature of the intervention as well as on its consequences and risks. The person concerned may freely withdraw consent at any time".*

concrete moment[38]. Nevertheless, article 8 of the Convention refers to emergency situations and establishes that when because of an emergency situation the appropriate consent cannot be obtained, any medically necessary intervention may be carried out immediately for the benefit of the health of the individual concerned.

The Explicatory Report of the Convention specifies that in emergencies, doctors may be faced with a conflict of duties between their obligations to provide care and seek the patient's consent. This article allows the practitioner to act immediately in such situations without waiting until the consent of the patient or the authorization of the legal representative where appropriate can be given. As it departs from the general rule laid down in Articles 5 and 6, it is accompanied by conditions. First, this possibility is restricted to emergencies which prevent the practitioner from obtaining the appropriate consent. The article applies both to persons who are capable and to persons who are unable either de jure or de facto to give consent. An example that might be put forward is that of a patient in a coma who is thus unable to give his consent (see also paragraph 43 above), or that of a doctor who is unable to contact an incapacitated person's legal representative who would normally have to authorize an urgent intervention. Even in emergency situations, however, health care professionals must make every reasonable effort to determine what the patient would want. Next, the possibility is limited solely to medically necessary interventions which can not be delayed. Interventions for which a delay is acceptable are excluded. However, this possibility is not reserved for life-saving interventions. Lastly, the article specifies that the intervention must be carried out for the immediate benefit of the individual concerned.

Thus, it can be concluded that the Oviedo Convention enforces informed consent, in an attempt to protect the human being against unwanted biomedical interventions. However, it can not be denied that it also includes significant exceptions to informed consent in those

[38]Article 6 – Protection of persons not able to consent

1. Subject to Articles 17 and 20 below, an intervention may only be carried out on a person who does not have the capacity to consent, for his or her direct benefit.
2. Where, according to law, a minor does not have the capacity to consent to an intervention, the intervention may only be carried out with the authorisation of his or her representative or an authority or a person or body provided for by law.
   The opinion of the minor shall be taken into consideration as an increasingly determining factor in proportion to his or her age and degree of maturity.
3. Where, according to law, an adult does not have the capacity to consent to an intervention because of a mental disability, a disease or for similar reasons, the intervention may only be carried out with the authorisation of his or her representative or an authority or a person or body provided for by law.
   The individual concerned shall as far as possible take part in the authorisation procedure.
4. The representative, the authority, the person or the body mentioned in paragraphs 2 and 3 above shall be given, under the same conditions, the information referred to in Article 5.
5. The authorisation referred to in paragraphs 2 and 3 above may be withdrawn at any time in the best interests of the person concerned.

cases where circumstances make it reasonable. It is also important to highlight that this Convention does not include specific references to data protection and privacy issues, as far as they fall in the scope of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 1981. Finally, it is important to remark that some of the EU Member States refused to sign the Oviedo Convention, including Germany, Austria or the United Kingdom. Some others, such as Sweden have not ratified it at the time this report is being redacted. Thus, its geographical scope is not at all as wide as in the case of the former Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.

9 INTERNAL REGULATION: THE "STATE OF EMERGENCY" DECLARATIONS.

In the former sections of this report, we have addressed both the main EU legislation and the conventions related to the Council of Europe which are currently ruling or about to start doing so on data protection and privacy issues. In general, these documents have been introduced in the national legal framework and developed to the different national laws embedding data normative issues in any way. In fact, the legal framework applicable in the EU countries usually follows a well-established pattern: it is the EU institutional architecture which settles the principles to be introduced in the national legislation through its legal tools and then it is the national authorities who take care of implementing these principles in their national context. This procedure works extremely well in normal circumstances.

However, it makes a sense to underline that, if we analyze the regulation applicable in case of CBRNE major crisis situation, we have to consider that many countries (at least those belonging to the continental legal tradition, as opposed to systems based on common law) do establish by mean of specific constitutional provisions, concrete regulations applicable to these ones. These are the so called states of alarm, emergency, "siege", martial law, etc[39].

The constitutional dispositions for those emergency situations do not normally include any express reference to the processing of personal data, but state important limitations to fundamental rights (including privacy and secrecy of communications, freedom of movements, etc.). By this mean relevant restrictions to the referred fundamental right

[39]For instance, article 103 of the Constitution the Kingdom of the Netherlands 2008, states that:

> 1. The cases in which a state of emergency, as defined by Act of Parliament, may be declared by Royal Decree in order to maintain internal or external security shall be specified by Act of Parliament. The consequences of such a declaration shall be governed by Act of Parliament.
>
> 2. Such a declaration may depart from the provisions of the Constitution relating to the powers of the executive bodies of the provinces, municipalities and water boards (waterschappen), the basic rights laid down in Article 6, insofar as the exercise of the right contained in this Article other than in buildings and enclosed places is concerned, Articles 7, 8, 9 and 12 paragraphs 2 and 3, Article 13 and Article 113 paragraphs 1 and 3.
>
> 3. Immediately after the declaration of a state of emergency and whenever it considers it necessary, until such time as the state of emergency is terminated by Royal Decree, the States General shall decide the duration of the state of emergency. The two Houses of the States General shall consider and decide upon the matter in joint session.

In the same sense, art. 48 of the Greece Constitution estates that:

> 1. In case of war or mobilization owing to external dangers or an imminent threat against national security, as well as in case of an armed coup aiming to overthrow the democratic regime, the Parliament, issuing a resolution upon a proposal of the Cabinet, puts into effect
>
> throughout the State, or in parts thereof the statute on the state of siege, establishes extraordinary courts and suspends the force of the provisions of articles 5 paragraph 4, 6, 8, 9, 11, 12 paragraphs 1 to 4 included, 14, 19, 22 paragraph 3, 23, 96 paragraph 4, and 97, in whole or in part. The President of the Republic publishes the resolution of Parliament. The resolution of Parliament determines the duration of the effect of the imposed measures, which cannot exceed fifteen days.

could be applicable allowing Public Authorities, for example, to access to personal data even without the consent of the data subject. These constitutional provisions referred to emergency situations (state of emergency, martial law, etc.) are, in many countries, legally developed in an specific Law or Act which empowers Public Authorities in such cases and for a limited period of time, to restraint the effectiveness of specific fundamental rights: among others, right to free circulation or right to privacy and secrecy of communications can be, during these concrete periods, importantly restricted. Nevertheless, it still remains a part of the data, for instance data related to biomedical research whose statute is not always completely clear. Initially, it seems difficult to accede to these data, as far as they are supposed to be used only for the purposed they were obtained. However, it is pretty difficult to guess if this assumption would prevail even in extreme circumstances when acceding to them seems to be the most promising way to find a solution in terms of national security, for instance[40].

Keeping this in mind, it can be noted that in extreme scenarios, it is very difficult to determine whether the right to data privacy should still prevail or be suspended, even in those cases when the EU legal framework provides us for a concrete solution, as far as national constitutions prevail against anything else. Furthermore, it is necessary to remind that the EU binding legislation includes clauses which allow Member States to regulate the exceptions to the data protection and privacy rights according to their own criteria and their adequacy to the circumstances existing. Thus, it is relevant to point out that even in those exceptional cases a limitation of the right to privacy (which is the one affected when processing personal data without the consent of the data subject) has to be specifically established by law on the basis of the constitutional dispositions existing on emergency situations.

In the next pages, we will have an excellent occasion to expose how these preventions have been addressed in four different EU Member States cases, Spain, France, Italy and Poland. We hope this annexed information to the main body of this report may serve as a reference.

[40]In order to be better understood, we will make an example. Suppose that we are in a moment when biomedical databases include the DNA data related to a significant percent of the population (which seems to be quite near in time). Imagine also that at any moment in that future we have to face a chain of bioterrorist attacks. The police finds biological samples that would probably pertain to the authors, but they do not match with the databases obtained from criminal offences investigations. Could the police or the army get access to biomedical databases in that cases? What if a state of emergency was declared?

10 CONCLUSIONS

Data management, data protection, and privacy concerns are likely to be a huge issue in CBRNE major crisis situations. Under those exceptional circumstances, these data are likely to be collected without the data subjects' consent, in highly stressful conditions, in the absence of normal infrastructure, and in the midst of political and legal uncertainty, which might result in serious attempts against fundamental human rights recognized in the EU Charter (art. 8). However, this does not mean that restrictions on rights related to severe crisis circumstances are not allowed at all. The EU legal framework, indeed, foresees this kind of limitations if needed be. The problem relays on defining what are the concrete limitations that the statement included in article 8 about fairness (*data must be processed fairly)* promote. In our opinion, this issue could be redefined as how to conciliate the defense of privacy and the protection of data with the protection of another relevant values, such as, for instance, security. This is precisely the role to be assumed by legislation developing the Charter, which distinguishes between the different type of data and the circumstances that might let the authorities to gain access to them, circumstances which include, as might be guessed, major crisis situations.

The main legal tool on this respect is the Directive 45/96/EC of the European parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Its main principles, transparency of data collection, fair and lawful processing, purpose limitation and specification, data minimization, consent, right to access, object, correct and withdraw one´s data, etc., correspond to the spirit of the Charter and already remain as the values to be addressed by a legislation which wants to reach an adequate protection of privacy. However, it is important to point out that this document allows the restriction of fundamental rights, such as informed consent when circumstances make it recommendable. In fact, article 8.4 Directive 45/96/EC states that subject to the provision of suitable safeguards, Member States may, for reasons of substantial public interest, lay down exemptions in addition to those laid down in paragraph 2 either by national law or by decision of the supervisory authority. CBRNE situations could be located in the previsions of article 8.4 Directive 45/96/EC allowing Member States on the basis of substantial public interests (public protection against disasters and emergency situations) to process even special categories of data (the ones revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership or concerning health or sex life) without the explicit consent of the data subject.

Nevertheless, it seems quite easy to sustain that lots of different technological

developments have occurred since the moment the Directive was passed till now. That is why it is about to be substituted by the Proposal for a Regulation of the European Parliament and of the Council of the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), dated on 25 January of 2012. This new regulation also includes exceptions to data protection and privacy rights. For instance, article 81 of the Regulation related to the processing of personal data concerning health disposes that it must be on the basis of Union law or Member State law which shall provide for suitable and specific measures to safeguard the data subject's legitimate interests, and be necessary for, among others, reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety, inter alia for medicinal products or medical devices or other reasons of public interest in areas such as social protection, especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system. Thus, laws will change, but the spirit remains the same. Same could be stated about Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 (Directive on privacy and electronic communications), which was adopted in 2002.

11 ANNEX 1 - A NATIONAL CASE STUDY: THE SPANISH CASE.

1.- The legal normative framework

In Spain, the existing regulation in the field of personal data processing is the Organic Law 15/1999, of 13th December, of Protection of Personal Data. In this field, relevant exceptions are established related to processing or accessing to personal data, when an emergency situation does occur.

As general rule article 6 Organic Law 15/1999 states that the processing of personal data requires the consent of the data subject, except when excluded by law. Nevertheless, the consent of the data subject is not necessary , among other reasons, when the personal data are collected for the performance of the functions of the Public Administrations in the field of their powers or when necessary in order to protect a vital interest of the data subject.

Similar exceptions are established for special categories of personal data in the Spanish regulation (article 7 Organic Law 15/1999). The basic criteria is that personal data revealing political opinions, religious or philosophical beliefs or trade-union membership can only be processed with the express and written consent of the data subject. Related to personal data revealing racial or ethnic origin and health or sex life they only can be collected, treated and transferred when, on the basis of the general interest, it is established in the law or the data subject expressly consents. Nevertheless, the processing of the referred special categories of data is possible when necessary for the sanitary assistance or medical treatments or the management of the sanitary services when the processing is made by a sanitary professional subject to professional secret.

Related to the communication of data (article 11 Organic Law 15/1999) the general rule is that it requires the previous consent of the data subject; nevertheless, the consent is not demanded, among others, when this transmission of personal data affects health data and it is necessary in order to solve an urgency which requires the access to them or so as to make epidemiologic studies as indicated in the national or autonomic legislation.

Finally and referred to transfer of personal data to third countries, the general principle is set in article 33 Organic Law 15/1999 which states that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if the third country in question ensures an adequate level of protection. As exception to the previsions of article 33, article 34 Organic Law 15/1999 establishes that by way of derogation from Article 33 a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection may take place on condition that, among others, the transfer is necessary or legally required on

important public interest grounds, or for the establishment, exercise or the transfer is necessary in for the prevention and medical diagnostic, the sanitary assistance or medical treatment or the management of sanitary services.

2.-The exceptional states in the Spanish Constitution

In Spain the Constitution of 1978 includes in its Part V (Relations between the Government and the Cortes Generales) a specific Section (116) devoted to State of alarm, State of Emergency and Martial Law (siege). According to Section 116 Spanish Constitution an Organic Act shall make provision for the states of alarm, emergency and siege (martial law) and the powers and restrictions attached to each of them. A state of alarm shall be proclaimed by the Government, by means of a decree agreed in Council of Ministers, for a maximum period of fifteen days. The Congress shall be informed and must meet immediately, and without its authorization the said period may not be extended. The decree shall specify the territory to which the effects of the proclamation apply.

A state of emergency shall be proclaimed by the Government by decree agreed in Council of Ministers, after prior authorization by the Congress. The authorization for and proclamation of a state of emergency must specifically state the effects thereof, the territory to which it is to apply and its duration, which may not exceed thirty days, subject to extension for a further thirty-day period, with the same requirements. A state of siege (martial law) shall be proclaimed by overall majority of Congress solely on the Government's proposal. Congress shall determine its territorial extension, duration and terms.

After the passing of the Spanish Constitution of 1978 an Organic Law (Organic Law 4/1981, of 1st June, regulating the states of Alarm, exception and siege –Martial Law–) that develops the previsions of the Spanish Constitution in this field. According to article 4 Organic Law 4/1981 the state of alarm could be declared when one of the following serious alterations of the normality do concur, in the whole or in one part of the national territory: catastrophe, calamities or public tragedies, sanitary crisis (epidemics or serious pollution situations), paralysis of public services which are essential for the community or shortage of essential products. Thus, it seems that the State of Alarm might be perfectly applicable in those cases when CBRNE major crisis situations merge.

The declaration of the State of Alarm allow the competent authorities to adopt a range of measures including: limiting the circulation or stay of persons or vehicles in concrete places and specific places, to practice the confiscation of all kind of goods and to impose personal obligatory services, to intervene and occupy temporarily industries, to restrain the use of services or the consumption of first necessity articles and to give the necessary orders

to ensure the supply of markets and the functioning of the services and production centers (article 11 Organic Law 4/1981). Additionally, and in case of catastrophe, calamities or public tragedies or sanitary crisis the competent authority can adopt not only the previous measures but also the ones previewed in order to fight against infectious diseases, the protection of the environment, in the field of water and applicable to forest fire (article 12 Organic Law 4/1981). Consequently, in case of declaration of a State of Alarm the Spanish legislation does not allow an indiscriminate access to personal data without the consent of the data subject. This means that, even if Spain were involved in a CBRNE major crisis situations, right to data protection and privacy will be respected, even if the restrictions and exceptions to their usual protection included in the EU and national legislation would be, of course, applicable.

The solution, however, could be different if it were the State of Exception to be declared. This kind of State can be declared when the free exercise of rights and liberties of the citizens, the normal functioning of the democratic institutions, of the community essential public services, or any other aspect of the public order, are so seriously affected that the exercise of the ordinary faculties would be insufficient so as to reestablish and maintain it. When an act of insurrection or force against the sovereignty or independence of Spain, its territorial integrity or the constitutional order has been produced or is about to be produced, the Government in accordance with article 116.4 Spanish Constitution can propose to the Congreso de los Diputados the declaration of the State of Siege (Martial Law).

The same solution might also happen in case of State of Exception or Siege (Martial Law) extraordinary measures can be adopted: among others, detention of persons if necessary for the maintenance of public order –suspension of article 17 Spanish Constitution– (article 16 Organic Law 4/1981), suspension of article 18.2 (inviolability of the home), 18.3 (secrecy of communications), 19 (free election of the place of residence and free move within the national territory), 21 (right to assembly and to demonstrate), 28.2 (right to strike) and 37.2 (right of workers and employers to adopt collective labour dispute measures) Spanish Constitution when the Congreso de los Diputados (Spanish Parliament) specifically allows it.

12 ANNEX 2 - A NATIONAL CASE STUDY: THE FRENCH CASE[41].

1.-Privacy and data protection: the French framework

France was one of the first European countries to adopt a data protection law. The Law on Informatics, Files, and Freedoms came into force in 1978. It was amended in 2004 in order to be brought into the line with, and give proper effect to the. The Law applies across the board to both the public and private sectors. More globally, Article 9 of the Civil Code addresses the right to the respect of privacy and Article 226-1 of the Penal Code defines sanctions when there is a breach of privacy, whatever the process involved.

According to the Law on Informatics, Files, and Freedoms, "Personal data" means any information relating to an identified or identifiable individual. An identifiable person is one who can be identified, directly or indirectly, in particular in reference to an identification number or to one or more specific elements related to his/her physical, physiological, mental, economic, cultural and social identity (e.g. name or first name, date of birth, biometrics data, etc.). The Law adds that "*in order to determine whether a person is identifiable, one should take into account the totality of the means allowing for identification which are in the possession of the controller* [person who determines the purpose and the means of the data processing] *or any person, or to which the controller or such other person may have access*."

Art. 6 of the Law stipulates that personal data must be "*collected and processed fairly and lawfully*" and "*for specified, explicit and legitimate purposes, and not further processed in a way incompatible with those purposes*."[42]All personal data must be collected in an adequate, relevant, and non-excessive way, in view of the purpose for which it is collected, and also be accurate, comprehensive and, when necessary, kept up to date. The Law provides that any individual must be informed of the reasons for the collection of information and may object to its processing either before or after it is collected.

The consent of the subjects is also required before processing personal data.[43]Implied consent of the data subject is sufficient for processing personal data, unless for certain kinds of information. Under the Law, express consent is required for any

[41]This annex is based on the information provided by FrédéricCoste, ElisandeNexon, from FRS, France. It has been slightly modified by the authors of the report in order to unify the whole text.

[42] The Law contains only one general exemption: "*processing carried out for the purpose of purely personal activities*".

[43]If consent is not given, personal data can only be processed if processing is necessary to do any of the following: Comply with a legal obligation to which the controller is subject ; Perform a contract to which the data subject is a party, or to take steps at the data subject's request before entering into a contract ; Protect the data subject's life ; Perform a public service duty entrusted to the data controller or the data recipient ; Pursue the data controller's or the data recipient's legitimate interests, provided this is compatible with the interests or the fundamental rights and liberties of the data subject.

processing of sensitive data[44] and for medical research requiring the collection of biological sample identifiers. The collection and processing of sensitive data are prohibited unless one of the following applies (*Article 8,* Law on Informatics, Files, and Freedoms):

.The data subject has given express consent.

.The processing is necessary to protect human life and the data subject is unable to give his consent.

.The processing relates to personal data made public by the data subject.

.The processing is necessary to establish, exercise or defend a legal claim.

In addition, the *Commission Nationale de l'Informatique et des Libertés*(CNIL) can authorize certain categories of processing, by taking into account its purpose if sensitive data is, within a short period of time, to be made anonymous using a procedure approved in advance by the Commission, Further, sensitive data processing is not prohibited if it is both:

.Justified by the public interest.

.Authorised by the CNIL or by a decree of the Council of State after a published opinion of the CNIL.

An independent administrative authority, the CNIL interprets and enforces the Law. It takes complaints, issues rulings, sets rules, conducts audits, makes reports, and ensures the public access to information being a registrar of data controllers' processing activities. CNIL is tasked with ensuring that information technology does not jeopardize human identity or breach human rights, privacy, as well as individual or public liberties. Its missions are to inform and assist individuals in the exercise of their rights and obligations, guarantees that citizens can access their personal data stored in processed files, keeps a list of notified data processing events, verifies compliance with the law, and regulates and controls.

- **Data protection rights**

Right of information: Every person may contact an organization directly to find out if he/she is listed or not by that organization in a data file.

Right of access: Every person may, on simple request addressed to the organization in question (and free of charge), have free access to all the information concerning him/her in clear language.

[44] Sensitive data is defined as data that reveals, directly or indirectly, the subject's racial or ethnic origins, political, philosophical or religious opinions, trade union affiliation, and health or sex life.

Right of rectification and deletion: Every person may directly require from the organization holding information about him/her that the data be corrected (if inaccurate), completed or clarified (if incomplete or equivocal), or updated (if obsolete) erased (if this information could not lawfully be collected).

Right of objection: Every person may oppose that information about him is used for advertising purposes or for commercial purposes.

He/she may also oppose to information concerning him/her being disclosed to a third party for such purposes.

Right of indirect access: Every person may request the CNIL to verify their personal data possibly recorded in records related to State security, national defense or public safety.

- **Data controllers' obligations**

Notify the file and its characteristics to the CNIL, except when exempted by the law or by the CNIL.

Ensure that citizens are in position to exercise their rights through information.

Ensure data security and confidentiality, to protect them from distortion or disclosure to unauthorized third parties.

Accept on-site inspections by the CNIL, and reply to any request for information.

The Law on Informatics, Files, and Freedoms adds that "*Nevertheless, further processing of data for statistical purposes or for purposes of scientific or historical purposes is deemed to be compatible with the purposes for which the data were initially collected*." Special chapters of the Law contain special rules on the processing of personal data in relation of the evaluation of medical practices and medical research.

12.1.-Exceptions to the general data protection and privacy rights in the French framework

- **State of emergency and exceptional circumstances**

The French legal framework takes into account the need to be able to address emergency situations such as accidents or disasters. Powers of the public administration are extended in this context.

Besides, several provisions exist and lay the framework for addressing exceptional situations. In the event of imminent danger arising from serious disturbances of public order or from events which by virtue of their nature and severity are deemed to be public disasters, Act n°55-385 of 3 April 1955 authorizes the Council of Ministers to proclaim by decree a state of emergency. Civil authorities are granted extended powers.[45] With the state of emergency (and the state of siege), prorogation beyond twelve days may only be authorized by law.

Article 16 of the French Constitution also authorizes the President of the Republic, after consultation of the Prime Minister, Presidents of the Assemblies, and Constitutional Council, to take measures required by circumstances, "[*w]hen the institutions of the Republic, the independence of the Nation, the integrity of its territory or the fulfillment of its international commitments are under serious and immediate threat, and when the proper functioning of the constitutional public powers is interrupted*".[46] Constitution Act n°2008-724 of 23 July 2008 brought democratic control on duration.[47]

A State of Emergency has been declared on one occasion over the last two decades, on 8th November 2005, in the context of a series of riots in French suburbs. It applied to 25 departments or parts of them, including the whole Île-de-France. Prorogation was then authorized by law. In December, 74 professors and lecturers of Law submitted a request for suspension to the Council of State. The Council then ruled that maintaining the State of Emergency was not "*an obvious illegality*". It was ended in early January.

Jurisprudence also sanctions the theory of exceptional circumstances[48]. The public administration is granted extended and derogatory powers, in order to be able to ensure the continuity of public services and abiding by the principle of legality is not possible. In such a context, public authority can for example suspend the application of a law or infringe on individual liberties[49]. This situation calls for a legality of exception and a strengthened

[45]By comparison with the state of emergency, the state of siege can be proclaimed, for the whole territory or part of it, after deliberation of the Council, by virtue of Article 36 of the 1958 French Constitution, in case of imminent peril resulting either from a foreign war or an armed insurrection. Police powers are then transferred from civil authorities to military authorities, if military authorities rule this transfer necessary.

[46] Constitution du 4 octobre 1958, article 16 (in French).

[47]After 30 days of exercising exceptional powers, the President of the National Assembly, the President of the Senate, 60 Members of the National Assembly or 60 Senators can appeal to the Constitutional Council. It will then assess whether the conditions still apply and its decision will be publicly announced. After 60 days and at any moment thereafter, the Council carries out such an assessment.

[48] Based on three main rulings: Council of State, "Heyriés", 28 June 1918 ; Council of State," Dames Dol et Laurent", 28 February 1919 ; Tribunal des conflits, "Dame de la Murette", 27 mars 1952.

[49] Council of State, "Heyriés", 28 June 1918, and "Rodes", 18 May 1983.

monitoring from the judge. These circumstances could be invoked in case of a war or a natural disaster. Article 16 of the Constitution is inspired by this theory.

- **Public health threat**

Law n°2004-806 of 9 August 2004 on public health policy createdin the Public Health Code a new preliminary chapter about serious health threats, in the title dealing with the fight against epidemics and some transmissible diseases. Law n°2007-294 of 5 March 2007 on the preparation of the health system to deal with large-scale health threats complemented the legal framework.

According to Article L3131-1of the Public Health Code (introduced by the 2004 Law), ”*in the event of a major health hazard requiring emergency action, in particular a possible epidemic, the Minister for Health may, by order with justification and in the interests of public health, prescribe measures proportionate to the risk incurred and appropriate to circumstances of time and venue, in order to prevent and limit the consequences of the potential threat on the health of the population*”, and the Minister may empower the territorially competent representative of the State to take all measures required for the implementation of these provisions, including individual measures. Administrative authorities can thus enforce healthcare measures on this basis. This legislation has for example been applied in the case of a patient refusing treatment against tuberculosis. It can thus offer an answer when patients with serious transmissible diseases refuse treatment, as this situation does not fall under the statutory exceptions to the principle of consent to medical treatment or the ”obligation to submit to care”, preventing the implementation of legally binding measures. However it should be noted that the opinion of the legal authority regarding the necessity and proportionality to the risks is still unknown[50].Article L 3110-2 states that justifications of measures taken in implementation of the above-mentioned article have to be periodically reviewed.

Outside these provisions, Article L3113-1 imposes to medical doctors and heads of services and of biomedical laboratories (public and private) a mandatory transmission of individual data to public authorities, either when a disease required an emergency local, regional or international action, or diseases the monitoring of which is necessary for public health policies (an order lists all these diseases).

The National Consultative Ethics Committee for Health and Life Sciences (CCNE) published an opinion about ethical issues raised by a possible influenza pandemic. It

[50]Bouvet R, Le Gueut M. Tuberculose et refus de soins: recours à la législation sur les menaces sanitaires graves, *Revue des Maladies Respiratoires*. 2013;30(6):451-457.

specifically draws attention to the risks of extending restrictions of fundamental liberties "*beyond what is strictly required to contain the influenza pandemic, either because of a maximalist (and therefore inappropriate) conception of the precautionary principle or as a demagogic concession*"[51]. It also reminds people that all rights and liberties that would not be specifically excluded should still be enforced. In this perspective, Articles L3131-1 specifies that the State representative at the level of the department and individuals under its authority have to protect the confidentiality of collected data on third parties.

Pandemic threats led to the promotion of business continuity plans. In 2009, to ease the process in the context of public health prevention, CNIL adopted an exemption from declaration regarding files compiling employees' personal information. Confidentiality had to be guaranteed (data given on a voluntary basis) and the access restricted to people in charge of human resources or involved in crisis management. These data had to be destroyed at the end of the pandemic alert[52].

Considering the issue of treatments and vaccinations, mandatory vaccinations may be seen as representing a dilemma as these obligations are in contradiction with the Article L1111-4 of the Public Health Code that requires a free and informed consent, whatever the medical act or treatment. Moreover, Articles 16-1 to 16-9 of the Civil Code impose the respect of the human body and the principle of its inviolability. Article L3131-1 nevertheless provides a solution in case of a serious health threat, as would also the theory of exceptional circumstances.

Regarding the specific question of smallpox, the Public Health Code lists measures that the Prefect[53] would be authorized to implement if a case was confirmed, including vaccination of exposed people and first responders, restricting movements of population, re-imposing border controls, as well as hospitalisation and isolation of individuals.

- **<u>The antiterrorist law and 2013 Military Programming Law</u>**

The Internal Security Code provides a legal framework that allows national police and gendarmerie services to access administrative automated processing of data and data hold by private operators, in the context of the prevention and fight against terrorism and threats to fundamental interests of the Nation (Article L222-1): access to the driver licenses database, the systems for the management of driver licenses, of identity cards, of passports,

[51]French National Ethics Committee for Health and Life Sciences, Opinion n°106: Ethical issues raised by a possible influenza pandemic, 2009.

[52]CNIL, Dispense n°14 – Délibération n°2009-476 du 10 septembre 2009 décidant la dispense de déclaration des traitements de données à caractère personnel mis en œuvre dans le cadre de plans de continuité d'activité relatifs à une pandémie grippale.

[53]The Prefect is the government representative at the levels of department and region.

of the files about foreign nationals, as well as data specified in the Code of Entry and Residence of Foreigner and the Right of Asylum.

Article 20 of the Military Programming Law allows authorized agents to access data, including in real-time, when individuals are suspected to pose a threat to national security or to the national scientific and economic potential, be involved in terrorist activities, to belong to an organized crime network or to movements seeking to undermine the institutions of the Republic[54].It creates Article L246-1 of the Internal Security Code. The secrecy of correspondence is otherwise guaranteed by Article 241-1.

The National Commission for the Control of Security Interceptions is an independent authority in charge of controlling the requests from State agencies regarding the collect of data.

- **Geo-localisation**

The National Assembly adopted on 28 March 2014 a law allowing geo-localisation in case of investigations about crimes or offences punished by at least three years of imprisonment. This procedure has to be authorized by the public prosecutor and judges. However it should be noted that this authorization is not required if geo-localisation is used to locate a victim thanks to his/her mobile phone, as it is in his/her own interest.

[54]Loi n°2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale.

13 ANNEX 3 - A NATIONAL CASE STUDY: THE ITALIAN CASE[55].

1.- Introduction: The State of Emergency and its implications in Italy

In the case of Italy, natural or man-made disasters are labelled into three different types. This distinction is essential, since it is related to the different ways of intervention organized by the Civil Protection Department. Therefore, according to their extension, their intensity and the response by the Civil Protection Department, natural and man-made disasters are classified as follows[56]:

- A Type (Municipal level), which entails the intervention of single administrations through ordinary measures. In this case, the mayor is responsible for addressing and coordinating the operational activities together with volunteer organizations;
- B Type (Regional and Provincial level), which involves the coordination of different local administrations of two or more municipalities through ordinary measures. In this case, the Prefect, the province and the region manage the crisis and coordinate the emergency response by assisting the affected population;
- C Type: (National level), which requires extraordinary means and power to be exercised for a limited period of time. Following the request of regional administration, the Council of Ministers declares a state of emergency. In this particular case, the Civil Protection Department assumes the coordination of response activities together with the prefect and regional, provincial and local administrations.

As a matter of fact, the Government can declare the "state of emergency" both before and after the occurrence of natural or man-made disasters. This declaration sets the limits, criteria and framework of intervention which, future ordinances issued by Civil Protection Department shall respect.[57] The "state of emergency" cannot last more than 180 days and it can be extended to other 180 days, under deliberation of the Council of Ministers (Art. 10 of Law Decree No. 93/2013 converted into Law No. 119, G.U. No. 242 of 15 Oct 2013).[58] The Declaration of "state of emergency" identifies the financial resources needed for the initial emergency interventions such as: assisting population, restoring the functionality of public services, as well as strategic infrastructure and reducing further risks.

[55]This annex is based on the information provided by Federica di Camillo, IstitutoAffariInternazionali – IAI, Rome. It has been slightly modified by the authors of the report in order to unify the whole text.

[56]Civil Protection Department, *Attivitàsuirischi* (Activities on Risks), http://www.protezionecivile.gov.it/jcms/en/rischi.wp.

[57] Civil Protection Department, Law no.100/2012, published in G.U. No.162 of 13/07/2012, *Dettaglio del Provvedimento*http://www.protezionecivile.gov.it/jcms/it/view_prov.wp;jsessionid=BB2A63E2A00B112121731F5CB715E76C?contentId=LEG34388.

[58] Law Decree No. 93/2013, converted into Law No.119 (G.U. No.242 of 15 Oct 2013)

http://www.gazzettaufficiale.it/eli/id/2013/08/16/13G00141/sg.

As far as "C type" events are concerned, the Council of Ministers declares the "state of emergency", under suggestion of the Head of Civil Protection Department. The state of emergency can also be declared upon proposal of the Undersecretary of State for the Presidency of the Council of Ministers and of the President of the Region.

Following the declaration, the Head of the Civil Protection Department takes "extraordinary powers" and related measures may be taken in derogation from the provisions in force. In particular, all crisis management activities are ruled by ordinances. Previously these ordinances were issued by the President of the Council of Ministers, while currently according to Law No. 100 of 2012[59] (G.U. No. 162 of 13 July 2012) the Head of the Civil Protection Department is charged with this power. There are two different types of ordinances:

- Ordinary ordinances
- Emergency ordinances

Overall, the ordinary ordinances deal with:

- Relief and assistance to population involved in the event;
- Securing both public and private buildings as well as cultural heritage seriously damaged and which can represent a threat for public and private safety;
- Restoration of the economic and productive infrastructure and networks essential for the recovery of normal conditions of life;
- Preventing situations which can threaten or damage people or things.

It is worth mentioning that, before these ordinances are issued, the Head of the Civil Protection Department must receive the needed documentation by the Regions hit by the natural and man-made disasters. Then, he/she can appoint a "Commissioner" who will write a report with a detailed list of all damages. This report is transmitted to the Council of Ministers which will evaluate the financial resources needed to restore the situation. Therefore, ordinances find the subjects responsible for the implementation of different interventions, according to their competences.

As far as financial procedures are concerned, ordinary ordinances issued within 30 days after the declaration of the "state of emergency" do not need the approval of the Ministry of Finances. After this time-span, they must be transmitted to the Ministry of Finances, whose approval is essential for the issuing of new ordinances.

[59]Law No.100 of 2012 (G.U. No. 162 of 13 July 2012), http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:2012-07-12;100.

The Council of Ministers can also decide to issue "emergency ordinances", in order to mobilize financial resources, through a specific Fund (the *Civil Protection Fund).* In addition, after the first emergency phase, the Government can decide, on the basis of the verification of the entity of the damage, to provide new financial resources for the recovery phase through law decrees. Every year, the Government refers to the Parliament about Civil Protection's activities, as well as about the criteria according to which *National Civil Protection Fund's* resources are used. In the case of an exceptional emergency that threatens the integrity of human life in a specific Region, the Head of the Civil Protection Department can ask the President of the Council of Ministers to use the national operational structures, after having informed the President of the Region involved in such disaster. In the case of great risk for human safety, the Head of Department can be asked to coordinate all the different activities (Art. 3 of Law No. 286/2002, G.U. No. 304 of 30 Dec 2002).[60]

As we stated before, State and Regions are not the only actors involved in this mechanism. Mayors play a pivotal role in local civil protection tasks, by managing and coordinating the activities dealing with rescue and assistance of their communities. Moreover, Law no.100/2012, stated that all municipalities would issue *Municipality emergency plans* by 90 after the issuing of the Law, according to the criteria set both by Regions and Civil Protection Department.

At least 10 days before the expiry of the "state of emergency" the Head of the Civil Protection Department issues another ordinance, in which the public administrations which will replace the Civil Protection in the management of the activities to overcome the critical situation provoked by the emergency, are defined.

These provisions are applied also in the case of natural or man-made disasters abroad. In this sense, in compliance with the principle of coordination with the competencies of the Ministry of Foreign Affairs, the Civil Protection Department may define the measures, approved by the President of the Council of Ministers, to declare state of emergency and to respond to disasters. (Art. 2 Law Decree No. 90/2005, converted into Law No. 152/2005, G.U. No. 176 of 30 July 2005).[61]

2.- The State of Calamity and its implications

[60] Law No. 286/2002 (G.U. No.304 of 30 Dec 2002) http://www.protezionecivile.gov.it/jcms/it/view_prov.wp;jsessionid=BB2A63E2A00B112121731F5CB715E76C?contentId=LEG21074.

[61] Law Decree No. 90/2005, converted into Law No.152/2005 (G.U. No.176 of 3 July 2005) http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legge:2005;90.

Art.1 of Law No. 996/1970 (G.U. No. 317 of 16 Dec 1970) defines "calamity" as an event which provokes the emergence of situations implying serious damage or danger for people's safety and their properties and which must be handled with technical extraordinary interventions.[62] In this context, Art. 2 of Law No. 225/1992 (G.U. No. 64 of 17 March 1992) makes a distinction between three different kinds of events:[63]

- Natural events or other events linked with man-made activity, which can be handled by single bodies or administrations which are competent in ordinary way.
- Natural events or other events linked with man-made activity, whose nature and extension imply a coordinated intervention by many bodies or administrations which are normally competent;
- Natural calamities, catastrophes or other events which due to their intensity and extension must be handled with extraordinary tools and powers.

The Italian legislation defines the case of calamity as the case in which exceptional natural events (for instance anomalies in the seasonal temperatures or precipitations) cause damage to productive activities. In particular, it refers to crises involving specific sectors, such as agriculture, trade, industry and craftsmanship. In such situations, Regions have the power to address the Government to ask for the recognition of the "state of calamity". The Council of Ministries will evaluate the request and, in the case it verifies the crisis, it will make the adequate decisions. Moreover, the Government can decide to appoint a "Commissioner", provided with extraordinary powers, who will coordinate those interventions needed to restore normality as soon as possible. As recently stated by the Civil Protection Department, even if industrial sector, trade and even craftsmanship, the "state of calamity" refers mainly to the agricultural sector.[64]

Therefore, the "state of calamity" is different from the "state of emergency" since it is linked to damages which affect specific sectors of human activity (agriculture, trade, industry and craftsmanship) whereas the "state of emergency" is usually declared in case of crisis affecting the majority of society structures. As far as normative considerations are concerned, the "state of calamity" is regulated by ordinary laws which set the entity of the financial intervention aimed to restore the previous situation.

We can distinguish between two different kinds of "state of calamity":

[62]Law No.996, published in G.U. No.317 of 16/12/1970, Http://Www.Normattiva.It/Uri-Res/N2ls?Urn:Nir:Stato:Legge:1970-12-08;996.

[63]Law no.225 of 24th of February 1992, published in G.U. No. 64 of 17/3/1992 http://www.protezionecivile.gov.it/cms/attach/editor/225_1992.pdf.

[64]**"Stato Di Emergenza e Stato Di CalamitàNaturale: DueStrumentiDiversi E Non Equiparabili",** ***IlGiornaleDellaProtezioneCivile, February 2014,***http://www.ilgiornaledellaprotezionecivile.it/?pg=1&idart=11521&idcat=2.

- State of calamity for damages to agriculture: according to Law No.185/1992 (G.U. No.51, of 2 March 1992), the Minister of Agricultural and Forestry Policies, in accordance with Regions, issues the Declaration on the "state of calamity".[65]
- State of calamity for damages to industry, trade and craftsmanship. In this context, the President of the Council of Ministers, under proposal from the Ministry of Industry and on the basis of a report issued by local Prefectures, issues the measures.

A *National Solidarity Fund* has been established, in order to support both public and private actors damaged by those calamities. Art. 2 of Law 185/1992 establishes that Regions, after verifying damages provoked by natural calamities, can ask within 60 days after the end of the event, the activation of those provisions for the restoring of the productive activity. The Ministry of Agriculture, in accordance with the Permanent Conference for the relations between State-Regions and Provinces, taking into consideration its financial exigencies, every three months issues a Decree in which both the amount of financial support, as well as the allocation of different resources every are established.[66]

3.-Quarantine

Quarantine is a term which refers to the separation and restriction of the movement of specific persons who may have been exposed to a communicable disease, in order to avoid the disease-spreading.[67] Quarantine implies the restriction of activities as well as the removal of people suspected – although not yet infected - as well as luggage, containers, transportations or freight, in order to avoid the contagion of the pathology. In this sense, quarantine is considered as a complementary tool within a more comprehensive strategy aimed at limiting illness-spreading both for acute and ordinary disease such as influenza.[68]

In the last years an important debate emerged in Italy about the possibility and the limitations for the use of *quarantine*. In the past, this tool was mainly applied to the so called "exotic diseases". However, the fact that its implementation represented a restriction of personal freedom became a strong argument for choosing other less rigid procedures. Therefore, this mechanism has been replaced by a simple "health monitoring", which consists of periodical pre-arranged medical examinations which eliminate the risk of limitation of personal freedom. This system is applied to those people who are coming from areas

[65] Law No.185/1992 (G.U. No. 51 of 2 March 1992), http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:1992-02-14;185.

[66] *Ibid.*

[67] Ministry of Public Health, Circular No.4 of 13 March 1998 http://www.trovanorme.salute.gov.it/norme/renderNormsanPdf?anno=0&codLeg=25185&parte=1%20&serie=.

[68] "Piano nazionale di preparazione e risposta ad una pandemia influenzale, *Centro nazionale per la Prevenzione e ilControllodelleMalattie del Ministerodella Salute*, http://www.epicentro.iss.it/focus/flu_aviaria/pianopandemico.pdf.

affected by epidemics and who are not vaccinated. Nonetheless, the *National Health Plan 2006-2008* states[69] that, on the basis of Decree of the President of Republic of the 7th of April 2006, international organizations, such as World Health Organization, can adopt binding norms dealing with some procedures such as quarantine, aimed to prevent the spreading of illnesses among member states.[70] In such sense, the Italian Health Regulation refers to the *International Health Regulation* issued in 2005.[71]

[69]Ministry of Public Health, *Piano sanitarionazionale 2006-2008,* http://www.salute.gov.it/imgs/C_17_pubblicazioni_1205_allegato.pdf.

[70] Decree of the President of Republic of 7 April 2006 (G.U. No.139 of 17 June 2006)

http://www.trovanorme.salute.gov.it/norme/dettaglioAtto?id=1114&completo=true.

[71] World Health Organization, *International Health Regulations 2005 2nd edition,* World Health Organization 2008 http://whqlibdoc.who.int/publications/2008/9789241580410_eng.pdf.

14 ANNEX 4 - A NATIONAL CASE STUDY: THE POLISH CASE[72].

Introduction

Polish legal order has provided feedback for transformation. It expresses values, the pursuit of which motivated social rejection of an unjust regime (the so called "real socialism"). These values include, among others, fundamental rights and freedoms. Rooting from socially recognized values system, Polish legal system makes the foundation of the rule of law (embracing democracy, respect for minority rights and the social market economy). Poland is a member of the transatlantic security community - a community-based on, and protecting the same values.

Constitutional regulations.

The Republic of Poland by the power of its Constitution confirms full respect for fundamental human rights and freedoms. These rights and freedoms include, among others, *Convention for the Protection of Human Rights and Fundamental Freedoms*, *Charter of Fundamental Rights of the European Union*,InternationalBillof Human Rights (i.e. *International Covenant on Civil and Political Rights, International Covenant on Economic, Social and Cultural Rights* and *Universal Declaration of Human Rights,*and other (European or universal) international agreements and commitments (such as OSCE).Constitutional catalog of fundamental rights and freedoms is contained in Chapter II of Polish Constitution (THE FREEDOMS, RIGHTS AND OBLIGATIONS OF PERSONS AND CITIZENS)[73]. Right to privacy,- especially important as regards data protection, is directly cited in Articles 47, 49, 51 of the Constitution.

However, the Constitution also regulates emergencies. The constitutional arrangements prove the desired expectations from the state of law derived from social experiences and expectations resulting from the "martial law" period 1981/1982. The Constitution diversifies emergencies, depending on their reasons, and attributes relevant special rights to the state administration and relevant to the needs restrictions on fundamental human rights and freedoms. The regulations are contained in Chapter XI EXTRAORDINARY MEASURES which include a range of articles related to emergency situations[74]. The most important of all of them is article 233.

[72]This annex is based on the information provided by Professor Jerzy Menkes, LL.D.The Main School of Fire Service: It has been slightly modified by the authors of the report in order to unify the whole text.

[73] The only presented values and freedoms are those directly, or indirectly, related to this study.

[74]*Article 228*

Article 233

1. The statute specifying the scope of limitation of the freedoms and rights of persons and citizens in times of martial law and states of emergency shall not limit the freedoms and rights specified in Article 30 (the dignity of the person), Article 34 and

1. In situations of particular danger, if ordinary constitutional measures are inadequate, any of the following appropriate extraordinary measures may be introduced: martial law, a state of emergency or a state of natural disaster.
2. Extraordinary measures may be introduced only by regulation, issued upon the basis of statute, and which shall additionally require to be publicized.
3. The principles for activity by organs of public authority as well as the degree to which the freedoms and rights of persons and citizens may be subject to limitation for the duration of a period requiring any extraordinary measures shall be established by statute.
4. A statute may specify the principles, scope and manner of compensating for loss of property resulting from limitation of the freedoms and rights of persons and citizens during a period requiring introduction of extraordinary measures.
5. Actions undertaken as a result of the introduction of any extraordinary measure shall be proportionate to the degree of threat and shall be intended to achieve the swiftest restoration of conditions allowing for the normal functioning of the State.
6. During a period of introduction of extraordinary measures, the following shall not be subject to change: the Constitution, the Acts on Elections to the Sejm, the Senate and organs of local government, the Act on Elections to the Presidency, as well as statutes on extraordinary measures.
7. During a period of introduction of extraordinary measures, as well as within the period of 90 days following its termination, the term of office of the Sejm may not be shortened, nor may a nationwide referendum, nor elections to the Sejm, Senate, organs of local government nor elections for the Presidency be held, and the term of office of such organs shall be appropriately prolonged. Elections to organs of local government shall be possible only in those places where the extraordinary measures have not been introduced.

Article 229

In the case of external threats to the State, acts of armed aggression against the territory of the Republic of Poland or when an obligation of common defence against aggression arises by virtue of international agreement, the President of the Republic may, on request of the Council of Ministers, declare a state of martial law in a part of or upon the whole territory of the State.

Article 230

1. In the case of threats to the constitutional order of the State, to security of the citizenry or public order, the President of the Republic may, on request of the Council of Ministers, introduce for a definite period no longer than 90 days, a state of emergency in a part of or upon the whole territory of the State.
2. Extension of a state of emergency may be made once only for a period no longer than 60 days and with the consent of the Sejm.

Article 231

The President of the Republic shall submit the regulation on the introduction of martial law or a state of emergency to the Sejm within 48 hours of signing such regulation. The Sejm shall immediately consider the regulation of the President. The Sejm, by an absolute majority of votes taken in the presence of at least half the statutory number of Deputies, may annul the regulation of the President.

Article 232

In order to prevent or remove the consequences of a natural catastrophe or a technological accident exhibiting characteristics of a natural disaster, the Council of Ministers may introduce, for a definite period no longer than 30 days, a state of natural disaster in a part of or upon the whole territory of the State. An extension of a state of natural disaster may be made with the consent of the Sejm.

Article 36 (citizenship), Article 38 (protection of life), Article 39, Article 40 and Article 41, para.4 (humane treatment), Article 42 (ascription of criminal responsibility), Article 45 (access to a court), Article 47 (personal rights), Article 53 (conscience and religion), Article 63 (petitions), as well as Article 48 and Article 72 (family and children).

2. Limitation of the freedoms and rights of persons and citizens only by reason of race, gender, language, faith or lack of it, social origin, ancestry or property shall be prohibited.

3. The statute specifying the scope of limitations of the freedoms and rights of persons and citizens during states of natural disasters may limit the freedoms and rights specified in Article 22 (freedom of economic activity), Article 41, paragraphs 1, 3 and 5 (personal freedom), Article 50 (inviolability of the home), Article 52, paragraph 1 (freedom of movement and sojourn on the territory of the Republic of Poland), Article 59, paragraph 3 (the right to strike), Article 64 (the right of ownership), Article 65, paragraph 1 (freedom to work), Article 66, paragraph 1 (the right to safe and hygienic conditions of work) as well as Article 66, paragraph 2 (the right to rest)".

Thus, Article233 of the Constitution is of crucial importance for the admissible restrictions of fundamental rights and freedom.

Emergencies statutory executive acts

Three Acts have been adopted for exercising extraordinary constitutional delegations in emergencies:

- Martial Law Act of 29 August 2002 on the Polish Armed Forces Supreme Commander's competence and his subordination to the state's constitutional authorities (Journal of Laws from 2002 no 156, item 1301, from 2003 no 228, item 2261, from 2004 no 107, item 1135);

- Act On State Of Emergency of 26 April 2002 (Journal of Laws from 2002 no 113, item 985, no 153, item 1271, from 2003 no 228, item 2261, from 2006 no 104, item 711, from 2011 no 222, item 1323, from 2013 item 628);

- Act On Natural Disaster of 18 April 2002 (Journal of Laws from 2002 no 62, item 558, no 74, item 676, from 2006 no 50, item 360, no 91, item 1410, from 2007 no 89, item 590, from 2009 no 11, item 59);

Martial Law Act specifies, inter alia, procedures of public authorities operation and rules of suspending and limiting human rights and freedoms during the martial law (Article 1). Martial law can be declared: "**Article 2. 1.** If there are external threats to the State, including those resulting from terrorist actions, armed attack on the territory of the Republic of Poland or, if the international agreement commits to a common defence against aggression. President of the Republic of Poland may, at the request of the Council of Ministers, impose martial law in parts or all of the territory of the state." The Council of Ministers is empowered to request the imposition of martial law and determine in the request, inter alia, the admissible limitations of human rights and freedoms. The President imposes Martial law by issuing regulation (Article 3) that specifies the admissible limitations of human rights and freedoms (to the law permitted extent).

The imposition of martial law (and its abolition) is notified to the Secretary General of the United Nations and the Secretary General of the Council of Europe by the Minister of Foreign Affairs.

A Province Governor directs the defence and civil defence tasks under martial law in respect not-reserved for other bodies, introduces and makes a request to other bodies to enter (ease and repeal) restrictions of human and civil rights and freedoms. Chapter 4 sets out the scope of freedoms and human and citizen rights limitations:

- all natural persons residing or staying there temporarily are subject to human and civil rights restrictions. Those restrictions shall apply to legal persons and organizations that do not have legal personality, established or operating on the territory under martial law covered (Article 18). Under martial law, among other things, communication, telecommunication and postal services may be limited, by requiring communication devices shutdown or services suspension for a limited period of time, as well as requesting to immediately deposit radio and TV broadcasting equipment and transceivers with the respective organs of state administration or otherwise safeguarding against its use jeopardising the state security or defence system and the right of access to public information (Article 24).

Article 1 of the **Act on state of emergency** specifies, among others, the range of limitations of freedoms and human rights in emergency. The Act specifies the mode of declaring / repelling the state of emergency, as well as the procedures for public authorities operation and the extent to limitations of freedoms and human rights.

State of emergency may be declared in Poland in the situation of threatening the constitutional system, public safety or public order (caused by, among others, terrorist activities or actions in cyberspace). State of emergency is declared by the President at the request of the Council of Ministers. The Act defines "cyberspace" as the space for processing

and exchanging information created by ICT systems, along with links between them and relationships with the users. The request indicates the area of the state of emergency imposition and, specifies restrictions to human rights and freedoms respective to threats. The Act specifies human rights restrictions. Citizens residing in the area of emergency and legal persons and organizations not having legal personality established or operating in the area are subjected to restrictions of human rights and freedoms.

Restrictions of human rights and freedoms should correspond to the nature and intensity of threats triggering the state of emergency, as well as provide an effective restoration of the state operations.

The imposition of martial law (and its abolition) is notified to the Secretary General of the United Nations and the Secretary General of the Council of Europe by the Minister of Foreign Affairs.

The **Act on natural disaster** provide for exclusive definition of the range of freedoms and human rights restrictions. Article 2 of the Act stipulates that "The state of emergency is imposed to prevent the effects of natural disasters or technical failures exhibiting characteristics of a natural disaster and to remove them". The legislator has clearly defined the terms, as follows:

- Force Majeur, as a natural disaster or a technical failure, the consequences of which threaten the life or health of a large number of persons, massively endanger property or the environment in large areas, while assistance and protection may be effectively provided exclusively under extraordinary measures, in co-operation of a number of organizations, institutions and specialized units and formations operating under a single command;

- the act of God, as an occurrence associated with the operation of the forces of nature, in particular, lightning, earthquakes, strong winds, heavy rainfall, long lasting extreme temperatures, landslides, fires, droughts, floods, ice phenomena on rivers, seas, lakes and water tanks, massive occurrence of pests, diseases of plants, animals or humans diseases or any other disastrous occurrence;

- technical failure as a violent, unexpected damage or destruction of a building, a technical device or system resulting in their use interruptions or their loss;

simultaneously pointing out that a natural disaster or technical failure may also be caused by terrorist action.

State of emergency is declared by the Council of Ministers regulation (on its own initiative or at the request of a competent province governor). The regulation specifies, inter alia, types of necessary restrictions of human and citizens rights. Restrictions are addressed

to residents of the area in which a state of emergency was imposed, legal persons and organizational units without legal personality established in that area. The referred above necessary restrictions (thus the boundaries of limitations set by the Council of Ministers) are introduced by local governments (a city, district or province mayor, or governor).

Declaration of the state of natural disaster, despite human rights and freedoms restrictions is not notified neither to the UN Secretary General nor the Secretary General of the Council of Europe.

Privacy Policy.

The legal basis of the statutory regulations regarding the protection of personal data is the Act on the Protection of Personal Data (Journal of Laws of 2002 no. 101, item 926, no. 153, item 1271, of 2004 no. 25, item 219, no. 33, item 285, of 2006 no. 104, item 708 and 711, of 2007 no. 165, item 1170, no. 176, item. 1238, of 2010 no. 41, item 233, no. 182 item 1228, no. 229, item 1,497, of 2011 no. 230, item 1371). The Act in conjunction with the regulation of the Constitution confirmed that "Article 1.1: Any person has a right to have his/her personal data protected".

2. Personal data processing can be carried out in the public interest, the interest of the data subject, or the interest of any third party, within the scope and subject to the procedure provided for by the Act". Pursuant to the regulation, solely this Act shall "determine the principles of personal data processing and the rights of natural persons whose personal data is or can be processed as a part of a data filing system". The Act shall apply to the processing of personal data in files, indexes, books, lists and other registers; computer systems, also in case where data is processed outside of a data filing system. Article 6 of the Act defines the terms of regulation: - personal data shall mean any information relating to an identified or identifiable natural person; an identifiable person is the 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/her physical, physiological, mental, economic, cultural or social identity).

Conclusions

In Polish law there is no regulation directly related to protection of personal data in emergency situations. As the catalogue of permissible restrictions of rights and freedoms during states of emergency is the closed catalogue, any limitation of protection is unacceptable.

Recommendations

In the event of a need to introduce a special regime for dealing with personal data in emergency situations, it is necessary to change - at least - statutory regulations.

15 ANNEX 5 - LIST OF RESOURCES.

1.- EU and International legislation

- Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding Supervisory Authorities and Transborder Dataflow (2001)
- Charter of Fundamental Rights of the European Union
- Communication from the Commission to the European Parliament and the Council of 24 June 2009 on Strengthening Chemical, Biological, Radiological and Nuclear Security in the European Union – an EU CBRN Action Plan
- Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 1981
- Convention on Human Rights and Biomedicine is a basic instrument at a regional European level related to the protection of Human Rights at the light of the new developments in the field of Biomedicine
- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 (Directive on privacy and electronic communications)
- Directive 45/96/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
- Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)
- 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 such as data
- Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, 13 December 2007

2.-Other sources:

- Consultation on the Commission's comprehensive approach on personal data protection in the European Union conducted from 4 November 2010 to 15 January 2011
- Consultation on the legal framework for the fundamental right to the protection of personal data, conducted from 9 July to 31 December 2009

- EPIC. “Council of Europe Privacy Convention”, at: http://epic.org/privacy/intl/coeconvention/
- EU Network Of Independent Experts On Fundamental Rights, *Commentary of the Charter of Fundamental Rights of the European Union*, June 2006, p. 91. Available at: http://llet-131-198.uab.es/CATEDRA/images/experts/COMMENTARY%20OF%20THE%20CHARTER.pdf
- European Court of Justice (ECJ) in the Lindqvist case law
- HEREDERO HIGUERAS, Manuel, *La directiva comunitaria de protección de los datos de character personal*, Aranzadi Editorial, Pamplona, 1997, 110.
- Special Eurobarometer 359, entitled Attitudes on Data Protection and Electronic Identity in the European Union