Rights, Equality and Citizenship (REC)

Programme of the EU Commission

(2014-2020)

MANDOLA

Monitoring and Detecting Online Hate Speech

D2.4a (intermediate)

Privact Impact Assessment of the MANDOLA outcomes

Abstract: The current report presents the method that has been designed in order to perform a Privacy Impact Assessment (PIA) of the MANDOLA outcomes.

Contractual Date of Delivery	30 February 2017
Actual Date of Delivery	11 July 2017
Deliverable Security Class	Public
Editor	Estelle De Marco
Quality and Ethical Assurance	Tatiana Synodiou

The *MANDOLA* consortium consists of:

FORTH	Coordinator	Greece
ACONITE	Principal Contractor	Ireland
ICITA	Principal Contractor	Bulgaria
INTHEMIS	Principal Contractor	France
UAM	Principal Contractor	Spain
UCY	Principal Contractor	Cyprus
UMO	Principal Contractor	France

Document Revisions & Quality Assurance

Internal Reviewer:

Tatiana Synodiou, Associate Professor, Law Department University of Cyprus, Chair of the Ethics Committee of Mandola.

Revisions

Version	Date	By	Overview
v.2.4a.0	16/06/2017	Inthemis (FR) Estelle De Marco as editor	Preparation of the report.
v.2.4a.1	27/06/2017	Inthemis (FR) Estelle De Marco as editor	Minor typo corrections and clarifications.
v.2.4a.2	11/07/2017	Inthemis (FR) Estelle De Marco as editor	Slight modifications and clarifications following Tatiana Synodiou's comments as quality assurance reviewer.

Table of Contents

List of Tables

1 Executive summary

A privacy impact assessment (PIA) has been defined in the PIAF EU project as "*a process for assessing the impacts on privacy of a project (…) or other initiative (...) and, in consultation with stakeholders, for taking remedial actions as necessary in order to avoid or minimise the negative impacts*"[1]. In this definition and in most of the other, very close, that have been provided by publications on this subject, the notion of "privacy" is largely understood, as referring to all the fundamental rights and freedoms that might be impacted by the aforesaid project or initiative, either without particular restriction or reducing the number of the targeted freedoms to those that might be impacted by a privacy and / or a data protection limitation[2].

Taking into account the importance of performing a PIA in the situations where projects are likely to present important risks for rights and freedoms, and the interrelations between PIA and the concept of privacy by design, this reports analyses the content of several PIA guidelines and methods in order to identify the steps to be included in the PIA MANDOLA method.

As a result, the proposed method includes seven steps that are detailed in Section 4 in order to prepare the PIA of the MANDOLA project outcomes.

[1] Paul De Hert, Dariusz Kloza, David Wright *et al.*, *Recommendations for a privacy impact assessment framework for the European Union*, PIAF (Privacy Impact Assessment Framework) project, Grant agreement JUST/2010/FRAC/AG/1137 – 30---CE---0377117/00---70, Deliverable D3, November 2012, p.5, available at http://www.piafproject.eu/Deliverables.html (last accessed on 15 June 2017).

[2] See for example Paul De Hert, Dariusz Kloza, David Wright *et al.*, *Recommendations for a privacy impact assessment framework for the European Union*, *op. cit.,* p. 14; Paul De Hert, "A Human Rights Perspective on Privacy and Data Protection Impact Assessments", *in* David Wright and Paul De Hert, *Privacy Impact Assessment*, Law, Governance and Technology Series volume 6, Springer, 2012, pp. 33 *et seq.*; Colin Colin Bennett's, *In Defence of Privacy*, Surveillance & Society, Vol. 8, No. 4, 2011, pp. 485–496, mentioned by Gary T. Marx, *Privacy Is Not Quite Like the Weather*, *in* David Wright and Paul De Hert, *Privacy Impact Assessment*, *op. cit.*, foreword p. vi.

2 Introduction

2.1 Background to the MANDOLA project

MANDOLA (Monitoring ANd Detecting OnLine hAte speech) is a 24-months project co-funded by the Rights, Equality and Citizenship (REC) Programme of the European Commission, which aims at making a bold step towards improving the understanding of the prevalence and spread of online hate speech and towards empowering ordinary citizens to report hate speech.

2.1.1 MANDOLA objectives

The MANDOLA specific objectives are the following:

- to monitor the spread and penetration of online hate-related speech in the European Union (EU) and in the EU Member States using big-data approaches, while investigating the possibility to distinguish, among monitored contents, between potentially illegal hate-related speech and non-illegal hate-related speech;
- to provide policy makers with actionable information that can be used to promote policies for mitigating the spread of online hate speech;
- to provide ordinary citizens with useful tools that can help them deal with online hate speech irrespective of whether they are bystanders or victims;
- to transfer best practices among EU Member States;
- to set-up a reporting infrastructure that will enable the reporting of potentially illegal hate speech.

The MANDOLA project addresses the two major difficulties in dealing with online hate speech: the lack of reliable data and the poor awareness on how to deal with the issue. Indeed, it is difficult to find reliable data that can show detailed online hate speech trends (inter alia in terms of geolocation and in relation to the focus of hate speech). Moreover, available data generally do not distinguish between potentially illegal hate speech and not illegal hate speech. In addition, the different legal systems in various Member States make it difficult for ordinary people to perceive the boundaries between both these categories of content. In this context, citizens might have difficulties to know how to deal with potentially illegal hate speech and how to behave when facing harmful but not illegal hate content. The lack of reliable data also prevents to make reliable decisions and push policies to the appropriate level.

The two MANDOLA innovations are (1) the extensive use of IT and big data to study and report online hate, and (2) the research on the possibility to make a clear distinction between legal and potentially illegal content taking into account the variations between EU Member States legislations.

MANDOLA is serving: (1) policy makers - who will have up-to-date online hate speech-related information that can be used to create enlightened policy in the field; (2) ordinary citizens - who will have a better understanding of what online hate speech is and how it evolves, and who will be provided with information for recognising legal and potentially illegal online hate-speech and for acting in this regard; and (3) witnesses of online hate speech incidents - who will have the possibility to report hate speech anonymously.

2.1.2 MANDOLA activities

In order to achieve the set up objectives the project envisages the following activities:

- An analysis of the legislation on illegal hate-speech at the European and international level and in ten EU Member States.
- An analysis of the applicable legal and ethical framework relating to the protection of privacy, personal data and other fundamental rights in order to implement adequate safeguards during research and in the system to be developed.
- The development of a monitoring dashboard, which aims to identify and visualise cases of online hate-related speech spread on social media (such as Twitter) and on the Web.
- The creation of a multi-lingual corpus of hate-related speech based on the collected data. It will be used to define queries in order to identify Web pages that may contain hate-related speech and to filter the tweets during the pre-processing phase. The vocabulary will be developed with the support of social scientists and enhanced by the Hatebase (http://www.hatebase.org/).
- The development of a reporting portal. It will allow Internet users to report potentially illegal hate-related speech material they have noticed on the Internet.
- The development of a smart-phone application. It will allow anonymous reporting of potentially hate-related speech materials noticed on the Web and in social media.
- The creation and dissemination of a Frequently Asked Questions document. It will be disseminated via the project portal and the smart-phone app.
- The creation of a network of National Liaison Officers (NLOs) of the participating Member States. They will act as contact persons for their country and will exchange best practices and information. They will also support the project and its activities with legal and technical expertise when needed.
- The development of a landscape of current responses to hate speech across Europe and of a Best Practices Guide for responding to online hate speech for Internet industry in Europe.

2.2 Purpose and scope of the report

The purpose of the current report is to present the method that will be used in order to perform a Privacy Impact Assessment (PIA) of the MANDOLA outcomes, the results of which will be presented in D2.4b. Sources and explanation of the choices that have been made in order to design this method will also be explained.

2.3 Document structure

The document is structured as follows.

Section 1 provides an executive summary.

Section 2 provides an introduction.

Section 3 defines the notion of PIA, identifies the sources that base the method and explain the choices that have been made.

Section 4 presents the method used in order to perform a PIA of the MANDOLA outcomes.

Section 5 provides a conclusion.

3 Notion, importance and content of a PIA

3.1 Notion and content of a PIA

Privacy Impact Assessments (PIA), as well as the concept of privacy by design which will be discussed further in Section 3.2.2., gained importance from the 1990's[3], as ethical tools aiming to ensure the efficiency of the legal instruments adopted from the 1970's in order to answer new concerns about privacy and personal data protection[4] (concerns that were themselves raised since the 1960s by the development of computer and network technologies[5]).

While PIA were - and still are - mainly a *"recommended step in the consideration and approval processes"*[6] of projects that can negatively affect privacy, their benefit and the increase of privacy concerns due to the further development of information and communication technologies (ICTs) led some countries to make them mandatory[7], followed by the new EU legislation. Indeed, data controllers will be required, in certain situations, to perform a Data Protection Impact Assessment (DPIA) under the new General Data protection Regulation (GDPR)[8] and Directive on personal data protection for the police and criminal justice sector"[9] (also called "Police Directive"[10]), which will be applicable in May 2018.

Differences of scope and targets might or might not exist between PIA and the latter (new) notion of DPIA, depending on the definition and methodology taken as a reference.

[3] See David Wright and Paul De Hert, *Privacy Impact Assessment*, Law, Governance and Technology Series volume 6, Springer, 2012, pp. 117 *et seq*.

[4] Examples of the Swedish data act enacted in 1973 and of the French data protection law enacted on 28th January 1978.

[5] See for instance Daniel J. Solove, *Understanding privacy*, Harvard University Press, 2008, especially p. 4; Nigel Waters, "Privacy Impact Assessment - Great Potential Not Often Realised*", in* David Wright and Paul De Hert, *Privacy Impact Assessment, op. cit.*, p.149; Adam Warren and Andrew Charlesworth, "Privacy Impact Assessment in the UK*", in* David Wright and Paul De Hert, *Privacy Impact Assessment, op. cit.*, p. 205.

[6] David Wright and Paul De Hert, *Privacy Impact Assessment, op. cit.*, p. 149.

[7] Nigel Waters, "Privacy Impact Assessment, Great Potential Not Often Realised"*, in* David Wright and Paul De Hert, *Privacy Impact Assessment, op. cit.,* p. 149.

[8] Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (known as the "General Data Protection Regulation" or "GDPR"), http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:FULL (last accessed on 12 May 2017).

[9] Directive (EU) 2016/680 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. In relation to the wording "Directive for the police and criminal justice sector", See for eample European Commission, *Reform of EU data protection rules*, http://ec.europa.eu/justice/data-protection/reform/index_en.htm (last accessed on 12 May 2017).

[10] European Commission - Fact Sheet, Questions and Answers - Data protection reform, 21/12/2015, http://europa.eu/rapid/press-release_MEMO-15-6385_en.htm (last accessed on 12 May 2017).

3.1.1 Definitions

A privacy impact assessment (PIA) has been defined in the PIAF EU project as "*a process for assessing the impacts on privacy of a project (…) or other initiative (...) and, in consultation with stakeholders, for taking remedial actions as necessary in order to avoid or minimise the negative impacts*"[11]. Roger Clarke defines a PIA as "*a systematic process that identifies and evaluates, from the perspectives of all stakeholders, the potential effects on privacy of a project, initiative or proposed system or scheme, and includes a search for ways to avoid or mitigate negative privacy impacts*"[12].

A PIA is therefore a tool that targets less the respect of a specific legislation than the respect of general requirements for protecting human rights and freedoms[13], through the assessment and mitigation of the impacts that an initiative can cause on these rights and freedoms. As a consequence, the assessment of these impacts may lead to determine safeguards that are not provided for by law, and even safeguards that aim to palliate the breach of a legal requirement that is difficult to apply in particular circumstances[14].

In these definitions and in most of the other, very close, that have been provided by publications on this subject[15], the notion of "privacy" is largely understood as referring to all the fundamental rights and freedoms that might be impacted by the aforesaid project or initiative, either without particular restriction or reducing the number of the targeted freedoms to those that might be impacted by a privacy and / or a data protection limitation[16].

A data protection impact assessment (DPIA) has been defined by the European Commission as "*a systematic process for evaluating the potential impact of risks where processing operations are likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes*"[17]. More recently, the Article 29 working

[11] Paul De Hert, Dariusz Kloza, David Wright *et al.*, *Recommendations for a privacy impact assessment framework for the European Union*, PIAF (Privacy Impact Assessment Framework) project, Grant agreement JUST/2010/FRAC/AG/1137 – 30---CE---0377117/00---70, Deliverable D3, November 2012, p.5, available at http://www.piafproject.eu/Deliverables.html (last accessed on 15 June 2017).

[12] Roger Clarke, *An Evaluation of Privacy Impact Assessment Guidance Documents*, International Data Privacy Law 1, 2 (March 2011) 111-120, available at http://www.rogerclarke.com/DV/PIAG-Eval.html (last accessed on 15 June 2017).

[13] See for instance Roger Clarke, *Privacy Impact Assessments*, 19 April 1999, last update on 26 May 2003, available at http://www.rogerclarke.com/DV/PIA.html (last accessed on 16 June 2017): "*A PIA (…) considers the impacts of a proposed action, and is not constrained by questions of whether the action is already authorised by law. Moreover, to the extent that relevant codes or standards exist, it does not merely accept them, but considers whether they address the public's needs*".

[14] Which might for example be the case of the principle of data minimisation, within the framework of a project aiming at performing big data analysis. See Section 3.2 of the current study.

[15] See for ex. David Wright and Paul De Hert, "Introduction to Privacy Impact Assessment*", in* David Wright and Paul De Hert, *Privacy Impact Assessment*, Law, Governance and Technology Series volume 6, Springer, 2012, pp. 3 *et seq.*, in particular pp. 5 *et seq.*

[16] See for example Paul De Hert, Dariusz Kloza, David Wright *et al.*, *Recommendations for a privacy impact assessment framework for the European Union*, *op. cit.*, p. 14; Paul De Hert, "A Human Rights Perspective on Privacy and Data Protection Impact Assessments", *in* David Wright and Paul De Hert, *Privacy Impact Assessment*, Law, Governance and Technology Series volume 6, Springer, 2012, pp. 33 *et seq.*; Colin Colin Bennett's, *In Defence of Privacy*, Surveillance & Society, Vol. 8, No. 4, 2011, pp. 485–496, mentioned by Gary T. Marx, *Privacy Is Not Quite Like the Weather*, *in* David Wright and Paul De Hert, *Privacy Impact Assessment*, *op. cit.*, foreword p. vi.

[17] EC recommendation of 9 March 2012 on preparations for the roll-out of smart metering systems (2012/148/EU), §I, 3 (c), available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:073:0009:0022:EN:PDF. The Article 29 Data Protection Working Party supports this definition: see Article 29 Data Protection Working Party, Opinion 04/2013 on the

party defined a DPIA as "*a process designed to describe the processing, assess the necessity and proportionality of a processing and to help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data (by assessing them and determining the measures to address them)*"[18]. More widely, some legal authors considers a DPIA as being "*an instrument to identify and analyze risks for individuals, which exist due to the use of a certain technology or system by an organization in their various roles (as citizens, customers, patients, etc.). On the basis of the outcome of the analysis, the appropriate measures to remedy the risks should be chosen and implemented*"[19].

Once again, in these definitions the notion of "risks" is understood as risks for privacy and personal data protection, covering other fundamental rights[20].

The aims of a PIA and of a DPIA are therefore the same (i.e. to evaluate the potential impacts of risks to rights and freedoms of a project or initiative, - which might be a personal data processing in the second case), to such an extent that these two instruments are often considered to be equivalents[21].

This being said, the two first DPIA definitions mentioned above create an important difference between a PIA and a DPIA. Indeed, on their basis, a DPIA is only supposed to assess the impact resulting from data processing operations, whereas a PIA will assess the impacts of a whole system or project that - potentially - includes data processing operations. This might lead to discover in a PIA some threats, rendered possible by the system, project or initiative and its context, that are not specifically linked with one of the projected personal data processing operations. In this sense, the scope of a PIA appears theoretically broader than the scope of a DPIA.

However, this last approach appears very restrictive and is not the one of the legal authors mentioned above. There is a temptation to agree with their conclusions since, if we define a DPIA by drawing an analogy with the preexisting notion of PIA, which is supposed to be the

Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems ('DPIA Template') prepared by Expert Group 2 of the Commission's Smart Grid Task Force (WP 205), adopted on 22 April 2013, p. 7, available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp205_en.pdf (URLs last accessed on 14 June 2017)

[18] Article 29 Data Protection working party, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*, WP248, 4 April 2017, p. 4, http://ec.europa.eu/newsroom/document.cfm?doc_id=44137 (last accessed on 15 June 2017).

[19] Felix Bieker, Michael Friedewald, Marit Hansen, Hannah Obersteller, and Martin Rost, "A Process for Data Protection Impact Assessment under the European General Data Protection Regulation", *in* K. Rannenberg and D. Ikonomou, *Privacy Technologies and Policy*, Fourth Annual Privacy Forum, APF 2016 Frankfurt. Heidelberg, New York, Dordrecht, London, available at http://www.springer.com/cda/content/document/cda_downloaddocument/9783319447599-c2.pdf?SGWID=0-0-45-1587701-p180200777 (last accessed on 15 June 2017).

[20] See for example CNIL, *Privacy Impact Assessments: the CNIL publishes its PIA manual*, 10 July 2015, PIA Manual 1 - Methodology, p. 3, https://www.cnil.fr/fr/node/15798 (last accessed on 15 June 2017): "*the term "privacy" is used as shorthand to refer to all fundamental rights and freedoms (including those mentioned in Articles 7 and 8 of the [EUCharter], Article 1 of the [Directive-95-46] and the Article 1 of the [DP-Act]: "human identity, human rights, privacy, or individual or public liberties*"); Article 35 of the GDPR evokes the "risk to the rights and freedoms of natural persons".

[21] see for ex. CNIL, *op. cit.* PIA Manual 1 - Methodology, p. 3: "*the acronym "PIA" is used interchangeably to refer to Privacy Impact Assessment (PIA) and Data Protection Impact Assessment (DPIA)*"; Article 29 Data Protection Working Party, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679* (WP248), 4 April 2017, http://ec.europa.eu/newsroom/document.cfm?doc_id=44137 (last accessed on 15 June 2017), p. 4: "*Note: the term "Privacy Impact Assessment" (PIA) is often used in other contexts to refer to the same concept*".

assessment of the impacts of an initiative on privacy, understood as covering impacts on all fundamental rights (at least those exercised in the private sphere[22]), a DPIA is supposed to consist as well in "*the identification of future consequences of a current or proposed action*"[23] on the right to personal data protection, understood as covering all fundamental rights (at least those exercised on the basis of a processing of personal data[24] and those being likely to be limited because of such a processing[25] - and more widely, since the data protection legislation refers to the protection of privacy - at least those exercised in the private sphere). The GDPR does not necessarily contradict such an approach, since even though it considers in its Article 35 that a DPIA is the assessment of the "*impact of the envisaged processing operations*", this must be done taking into account "*the nature, scope, context and purposes of the processing*" - which means that the GDPR may implicitely command to assess the impacts of the whole context of the processing operations (on several privacy and other fundamental rights aspects, including on personal data that are not intended to be processed but that might be processed due to a project misuse). This might extend the scope of the assessment to all the impacts of the project, system or initative, as soon as existing or non existing[26] personal data might be affected due to the functionning or even the existence of this system. In such an approach, a PIA and a DPIA are equivalent terms, but their meaning go beyond the definitions provided by the European Commission and the Article 29 data protection working party.

3.1.2 Guidelines and methods

There is currently no undisputed standard to conduct a PIA or a DPIA. First PIA guidelines emerged in the 1990[27], notably on the initiative of several government agencies and data protection authorities[28], and several methods currently coexist. In this regard, the research consortium of the PIAF project - which aimed to encourage the EU and Member States to adopt a progressive PIA policy[29], has conducted in its first report a very interesting analysis

[22] Such as for example the right to freedom of expression, the right to freedom of assembly, and the right to non-discrimination. More globally, if we consider that the protection of privacy encompasses the right to personal data protection, rights concerned are all the rights that have been studied in the MANDOLA deliverable D2.2 - Identification and analysis of the legal and ethical framework, MANDOLA project (Monitoring ANd Detecting OnLine hAte speech) - GA noJUST/2014/RRAC/AG/HATE/6652, http://mandola-project.eu/, 12 July 2017.

[23] This formula corresponds to the definition given to an impact assessment by the International Association for Impact Assessment (IAIA): see Roger Clarke, *Privacy Impact Assessments*, 19 April 1999, last update on 26 May 2003, available at http://www.rogerclarke.com/DV/PIA.html (last accessed on 16 June 2017), "Origins and definition".

[24] Such as, for example, the freedom to conduct a business, the right to a fair trial, the freedom of expression, the freedom of assembly. See the MANDOLA deliverable D2.2 - *Identification and analysis of the legal and ethical framework*, *op. cit.*

[25] Such as, for example, the right to freedom of movement, the right to liberty and security, the right to presumption of innocence and to a fair trial, the right to freedom of expression, the right to freedom of assembly and the right to non discimination. See the MANDOLA deliverable D2.2 - *Identification and analysis of the legal and ethical framework*, *op. cit.*

[26] A project might for example lead to self-censorship of Internet users, and therefore prevent individuals from releasing some information online.

[27] Paul De Hert, Dariusz Kloza, David Wright *et al.*, *Recommendations for a privacy impact assessment framework for the European Union*, PIAF (Privacy Impact Assessment Framework) project, Grant agreement JUST/2010/FRAC/AG/1137 – 30--CE--0377117/00--70, Deliverable D3, November 2012, p.5, available at http://www.piafproject.eu/Deliverables.html (last accessed on 15 June 2017).

[28] See for ex. Roger Clark, *Privacy Impact Assessment: Its Origin and Development*, *in* Computer Law & Security Review 25, 2 (April 2009), pp. 123-135, http://www.rogerclarke.com/DV/PIAHist-08.html (last accessed on 15 June 2017).

[29] This project has ended in October 2012.

of the PIA methods of seven countries (Australia, Canada, Honk-Kong, Ireland, New-Zealand, United Kingdom, United States), and of 10 PIA case studies[30]. The PIAF project has moreover proposed the construction of a model framework applicable to the EU[31] and some projects have developed their own method, as the VIRTUOSO EU project[32] and the ePOOLICE EU project[33] did.

As regards guidelines, a norm ISO 29134 related to PIA is under development. At the EU level, a Privacy and Data Protection Impact Assessment Framework for RFID Applications has been published in January 2011, and a Smart Grid DPIA template has been produced by the Expert Group 2 of the European Commission Smart Grid Task Force, and submitted early 2013 to the Article 29 Data Protection Working Party's and the Council of European energy regulator's opinions[34]. More recently, the Article 29 Data Protection Working Party published guidelines to perform a DPIA[35] taking into account the new EU legislation[36], the latter (which impose the performance of a data protection impact assessment in certain cases) providing for elements that must at least be included in a DPIA.

Along with these PIA and DPIA guidelines that apply specifically to privacy risks (including generally the issue of personal data protection) or to personal data risks (including generally the issue of privacy protection), both including most of the time the issue of the protection of the data subject's or the privacy subject's fundamental rights and freedoms more globally (either linked or not to the right to privacy or to personal data protection), the ENISA emerging and future risks framework (2010)[37] provides for risk management and risk assessment guidelines inspired by international standards, as well as some government agencies such as the French ANSSI[38] which proposes the EBIOS method[39]. Most of the PIA

[30] David Wright, Kush Wadhwa, Paul De Hert, Dariusz Klova, *A Privacy Impact Assessment Framework for data protection and privacy rights*, PIAF (Privacy Impact Assessment Framework) project, Deliverable D1, 21 Sept. 2011, available at http://www.piafproject.eu/Deliverables.html (15 June 2017).

[31] *Ibid.*

[32] Gabriela Bodea, Marc van Lieshout, Linda Kool, Leo van de Wees, *D03.01.01 - A privacy impact assessment framework for the use of open source information in border control and security*, VIRTUOSO EU project (Versatile InfoRmation Toolkit for end-Users oriented Open-Sources explOitation), project number FP7-SEC-GA-2009-242352, Deliverable D3.1.1 (WP 3 - Privacy, ethical and legal aspects), 31 October 2010, available on http://www.virtuoso.eu/VIRTUOSO/servlet/document.listPublic (last accessed on 15 June 2017).

[33] Estelle De Marco *in* Estelle De Marco*,* Nasredine Semmar *et al.*, *Deliverable D3.4 - Final report*, ePOOLICE project (early Pursuit against Organized crime using envirOnmental Scanning, the Law and IntelligenCE systems), projet n° FP7-SEC-2012-312651, version 1.4 of 28 December 2015 (Doc. ID EPO-1512-WP03-004-V1.4-DV-RE), Section 4 and Annex 1, https://www.epoolice.eu/ (last accessed on 15 June 2017).

[34] See the Article 29 Data Protection Working Party, Opinion 04/2013 on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems ('DPIA Template') prepared by Expert Group 2 of the Commission's Smart Grid Task Force (WP 205), adopted on 22 April 2013, esp. footnote n°7 p. 3, available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp205_en.pdf (last accessed on 14 June 2017).

[35] Article 29 Data Protection working party, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*, WP248, 4 April 2017, p. 4, http://ec.europa.eu/newsroom/document.cfm?doc_id=44137 (last accessed on 15 June 2017).

[36] Namely the GDPR and the Directive on personal data protection for the police and criminal justice sector.

[37] ENISA website, Risk management, available at http://www.enisa.europa.eu/activities/risk-management (last accessed on 15 June 2017).

[38] Agence nationale de la sécurité des systèmes d'information (National agency for information systems security).

[39] EBIOS 2010, Expression des Besoins et Identification des Objectifs de Sécurité, ANSSI, 25 October 2011, available at https://www.ssi.gouv.fr/guide/ebios-2010-expression-des-besoins-et-identification-des-objectifs-de-securite/ (in French).

and DPIA guidelines refer more or less directly to these risk management standards in order to perform the risk assessment which forms part of the PIA or DPIA. For exemple, we can mention the PIA guidelines produced by the French data protection authority (CNIL)[40], which refer explicitly to the EBIOS method, even though the scope of this assessment method is very reduced since it is restricted to the risks that might threaten the personal data that are processed, without having regards to the risks caused to other fundamental rights as assets, either as a result of processing operations or as a result of the existence or the functioning of the whole system beyond what strictly relates to personal data processing operations.

The analysis of all the above-mentioned works and guidelines relating to PIA and DPIA enables to identify seven fundamental steps whose content should be included in a PIA, which will be understood in our study in a broad sense while maintaining a link with privacy and personal information**. As a result, the notion of PIA will be understood as including the assessment of risks posed by a project to the right to private life and to personal data protection, and more widely to the other rights and freedoms either exercised by individuals in their respective personal spheres, or restricted by extension because of a privacy limitation or a personal data use**[41].

These seven fundamental steps will be analysed in Section 3.4 of the current study.

3.2 Importance of a PIA and links with privacy by design

3.2.1 The importance to perform a PIA

Technologies[42] such as cloud computing, big data, big analytics, and ambient intelligence, and new uses such as social networking, create new risks for privacy, data protection, and other fundamental rights including freedom of expression[43], presumption of innocence, right

See also an overview in English at https://www.ssi.gouv.fr/archive/en/confidence/documents/methods/ebiosv2-methode-plaquette-2003-09-01_en.pdf (URLs last accessed on 15 June 2017).

[40] CNIL, *Privacy Impact Assessments: the CNIL publishes its PIA manual*, 10 July 2015, https://www.cnil.fr/fr/node/15798 (last accessed on 15 June 2017). See also David Wright and Paul De Hert, "Introduction to Privacy Impact Assessment*", in* David Wright and Paul De Hert, *Privacy Impact Assessment*, Law, Governance and Technology Series volume 6, Springer, 2012, pp. 3 *et seq.*, in particular pp. 10 *et seq.*

[41] An example provided by the Article 29 Data Protection Working Party is the financial loss that could result from inaccurate billing or price discrimination, which may be caused by a personal data processing (Article 29 Data Protection Working Party, Opinion 04/2013, *op. cit.*, p. 7). Another example could be a (even temporary) deprivacy of liberty due to an investigation targeting someone other than the perpetrator of a penal offence, opened on the basis of the processing of non-reliable personal data.

[42] The current Section is based on Estelle De Marco previous works in Estelle De Marco *in* Estelle De Marco *et al.*, Deliverable D3.3 - Legal recommendations - ePOOLICE project (early Pursuit against Organized crime using envirOnmental Scanning, the Law and IntelligenCE systems), projet n° FP7-SEC-2012-312651, version 1.3 of 10 December 2014, Section 3.3, available at https://www.epoolice.eu/ (last accessed on 15 June 2017).

[43] Regarding social networking, see the Recommendation CM/Rec(2012)4 of the Council of Europe Committee of Ministers to Member States on the protection of human rights with regards to social networking services, 4 April 2012, https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805caa9b (last accessed on 15 June 2017). Regarding more specifically ambient intelligence, see Paul De Hert, Serge Gutwirth, Anna Moscibroda, David Wright, and Gloria González Fuster, *Legal Safeguards for Privacy and Data Protection in Ambient Intelligence*, first online on 7 October 2008, Personal and ubiquitous computing August 2009, Volume 13, Issue 6, pp. 435-444, https://link.springer.com/article/10.1007/s00779-008-0211-6 (last accessed on 16 June 2017).

to non-discrimination, freedom of assembly, freedom of movement, right to liberty and security, and freedom to conduct a business[44]. Indeed,

- These technologies tend to imply by default the recording of a maximum of data, while the EU legal instruments protecting personal data require, on the opposite, a minimisation of the collected data[45].
- These technologies tend to imply the collection of this large amount of data without determining a precise purpose for this collection, since the database thus constituted is designed to enable subsequent processing with different purposes which will be determined after the data collection. This situation comes into conflict with the principle of legitimate, specified, and explicit purpose (which includes the principle of compatible use[46]).
- These technologies have weaknesses, implying notably risks of identity theft, of malicious attacks, of lack of personal control over the technologies[47], and of illegitimate access and use[48].
- These technologies and uses increase surveillance and profiling possibilities (notably through data-mining), which may severely infringe the above-mentioned freedoms, primarily the right to the secrecy of private life and to personal data protection:
    - Web scanning, including social networks scanning, may be seen as a disproportionate interference into the right to privacy (and more precisely to informational privacy in the opinion of some legal authors[49]), due to the "*nature of the activity being affected*"[50]. Indeed, individuals who publish information on the

[44] See Estelle De Marco *et al.*, MANDOLA deliverable D2.2 - *Identification and analysis of the legal and ethical framework*, MANDOLA project (Monitoring ANd Detecting OnLine hAte speech) - GA noJUST/2014/RRAC/AG/HATE/6652, http://mandola-project.eu/, 12 July 2017. See also article 29 Data Protection Working Party, *Statement on the role of a risk-based approach in data protection legal frameworks* (WP 218), 30 May 2014, p. 4, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf (last accessed on 15 June 2017).

[45] See for instance Antoinette Rouvroy, "Privacy, Data Protection, and the Unprecedented Challenges of Ambient Intelligence", in *Studies in Ethics, Law and Technology*, Volume 2, Issue 1, 2008, Article 3, p. 39, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1013984 (last accessed on 15 June 2017).

[46] See Estelle De Marco *et al.*, MANDOLA deliverable D2.2 - *Identification and analysis of the legal and ethical framework*, *op. cit.*, Section 4.2.3.3.2.3.

[47] Michael Friedewald, Elena Vildjiounaite, Yves Punie and David Wright, *Privacy, identity and security in ambient intelligence: A scenario analysis*, December 2005, *in* Telematics and Informatics, 2007, vol. 24, pp.15-29.

[48] Noël Chahid-Nourai (former member of the French data protection Authority), intervention à la table ronde « Secret et nouvelles technologies » (speech at the round table entitled "secrecy and new technologies"), colloque consacré au secret professionnel organisé par la Conférence des bâtonniers (seminar on professionnal secrecy organised by the Conference of the Bar Presidents), Les petites affiches, n° 122, 20 June 2001, p. 25 *et seq.*: "*even in most decent and commendable government agencies, there are temptations, weaknesses, fragilities*" (translated from French: « *même dans les corps de l'Etat les plus estimables et les plus respectables, il y a des tentations, des faiblesses, des fragilité* »).

[49] See for example Anne Gerdes, who defines informational privacy as "*individuals' ability to control the flow of personal information, including how information is exchanged and transferred*": Anne Gerdes, "Privacy preserving Design Framework in relation to an Environmental Scanning System for *Fighting Organized Crime*", in K. Kimppa, D. Whitehouse, T. Kuusela, J. Phahlamohlaka (Eds.), *ICT and Society*, 11th IFIP TC 9 International Conference on Human Choice and Computers, HCC11 2014, Turku, Finland, 30th July - 1st August 2014, Proceedings, Series IFIP Advances in Information and Communication Technology, Vol. 431. The author refers to H. Tavani, "*Informational privacy, data mining, and the internet*", Ethics and Informational Technology, 1, 137-145 (1999).

[50] See Estelle De Marco *et al.*, MANDOLA deliverable D2.2 - *Identification and analysis of the legal and ethical framework*, *op. cit.*, Section 4.1.3., proportionality, on the "*proportionality of the restricted behaviour*".

internet in several different contexts expect the respect of each of these contexts. In other words, they did not expect and consent neither to the collection of their pieces of information out of their original context, nor to the combination of all their published information, all contexts taken together.

- Data mining techniques aim at "*predicting individual behaviours and preferences with more accuracy and impartiality than allowed by human adjudication*"[51]. Especially, "*automated data linkages*" can be created "*between seemingly non-identifiable data*", leading to "*a broad portrait of an individual*" which was "*once inconceivable since the identifiers were separated in various database*"[52].Therefore, these technologies lead to create information and to "*produce knowledge*"[53], on a given individual, without that person knowing it, in addition to enable a high transparency of this individual *vis-à-vis* the data's controller or any person authorised to access these data.
- Big Data enables to connect "*key pieces of data that connect people to things*", converting anonymous data into personal data information "*revealing details about a person's lifestyle and habit*"[54].
- Other freedoms may be impacted, such as the freedom to communicate or to make certain choices, since, for example, individuals under surveillance may self-censor their publications. Surveillance and profiling may also lead to incorrect categorisation, loss of autonomy, discrimination and stigmatisation[55].

These new risks raise primarily the questions of the personal control over one's own data and content of several fundamental rights such as private life and freedom of expression, and, within the framework of the MANDOLA project, of the legitimacy of certain actions such as online scanning and potential recommendations to penalise certain kind of behaviours.

These issues may call for new or specific safeguards, as it has been already analysed by several legal authors[56]. Identifying such safeguards where they are needed is the express purpose of a PIA, reason for which such an initiative is more important than ever where a project, especially of a technological nature, presents risks for rights and freedoms (and

[51] Antoinette Rouvroy, "Privacy, Data Protection, and the Unprecedented Challenges of Ambient Intelligence", in *Studies in Ethics, Law and Technology*, Volume 2, Issue 1, 2008, Article 3, p. 39, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1013984 p. 2 (last accessed on 15 June 2017).

[52] Ann Cavoukian, David Stewart, Beth Dewitt, *Using Privacy by Design to Achieve Big Data Innovation Without Compromising* Privacy, 10 June 2014, p.11, available at https://gpsbydesign.org/resources-item/using-privacy-by-design-to-achieve-big-data-innovation-without-compromising-privacy/ (last accessed on 15 June 2017).

[53] Antoinette Rouvroy, "Privacy, Data Protection, and the Unprecedented Challenges of Ambient Intelligence", *op. cit*., p. 13 of the electronic version.

[54] Ann Cavoukian, David Stewart, Beth Dewitt, *Using Privacy by Design to Achieve Big Data Innovation Without Compromising Privacy*, *op. cit*., p.11.

[55] Mireille Hildebrandt and Bert-Jaap Koops, "The challenges of Ambient Law and legal protection in the profiling era", May 2010, Modern Law Review 73 (3), p. 428-460; Recommendation CM/Rec(2012)4 of the Council of Europe Committee of Ministers to Member States on the protection of human rights with regards to social networking services, 4 April 2012, https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805caa9b (last accessed on 15 June 2017).

[56] Paul De Hert, Dariusz Kloza, David Wright *et al*., *Recommendations for a privacy impact assessment framework for the European Union*, PIAF (Privacy Impact Assessment Framework) project, Grant agreement JUST/2010/FRAC/AG/1137 – 30---CE---0377117/00---70, Deliverable D3, November 2012, p.5, available at http://www.piafproject.eu/Deliverables.html (last accessed on 15 June 2017); Mireille Hildebrandt and Bert-Jaap Koops; *op. cit*.

beyond the fact that a P/DPIA will be mandatory in 2018, in relation with personal data processing where the latter will be likely to result in a high risk for rights and freedoms).

3.2.2 Privacy by Design

The privacy by design concept has been developed by Dr. Ann Cavoukian, former Information and Privacy Commissioner of Ontario[57].

This concept has been considered as being the "*next* (which we could replace by "new") *generation of privacy protection*"[58], to respond to new challenges posed by technology. It is partly based on the recognition that, in the current technological context, "*meaningful informational self-determination is becoming increasingly difficult to achieve*"[59] and that privacy protection is becoming a "*business issue*", since it is becoming "*an important aspect of an organization's ability to inspire and maintain consumer confidence, trust, and loyalty*"[60]. Therefore, privacy protection - or, at least, compliance with legal rules protecting privacy - should not be seen as a burden that threatens business and innovation, but as a "*win-win, positive-sum approach*"[61]. The objective of privacy by design is indeed to obtain a deep and meaningful respect of privacy by embedding its requirements "*into the design specifications of information technologies, business practices, and networked infrastructures as a core functionality*", while "*preserving a commitment to full functionality*"[62], and serving the organisation's interests (by improving customers' or citizens' confidence, reducing the risk of liability associated with privacy breaches, cost saving…)[63].

This privacy by design approach contains seven principles, which, for a part of them, mostly call for the application of legal and ethical rules as they already exist at the EU level, while the others mostly intend to govern the implementation of privacy solutions, after completion of an impact study. These principles are the following:

- ✓ **Proactive, not reactive:** privacy by design aims at preventing privacy infringments, by anticipating risks before they happen, and not to offer remedies to privacy risks already materialised. The approach is therefore proactive.
- ✓ **Privacy as the default setting:** privacy by design aims at protecting individuals without requiring any action from these individuals. Privacy protection is "*built into the system*"[64] and therefore automatically ensured.

[57] The current Section is based on Estelle De Marco previous works in Estelle De Marco *in* Estelle De Marco *et al.*, Deliverable D3.3 - Legal recommendations - ePOOLICE project (early Pursuit against Organized crime using envirOnmental Scanning, the Law and IntelligenCE systems), projet n° FP7-SEC-2012-312651, version 1.3 of 10 December 2014, Section 3.2.2., available at https://www.epoolice.eu/ (last accessed on 15 June 2017).

[58] Ann Cavoukian, *Privacy by Design in Law, Policy and Practice*, *A White Paper for Regulators, Decision-makers and Policy-makers*, August 2011, p. 10, available at https://gpsbydesign.org/resources-item/privacy-by-design-in-law-policy-and-practice-a-white-paper-for-regulators-decision-makers-and-policy-makers/ (last accessed on 15 June 2017).

[59] Ann Cavoukian, *Privacy by Design in Law, Policy and Practice*, *op. cit*., p. 6.

[60] Ann Cavoukian, *Privacy by Design in Law, Policy and Practice*, *op. cit*., p. 8.

[61] Ann Cavoukian, *Privacy by Design in Law, Policy and Practice*, *op. cit*., p. 10.

[62] Ann Cavoukian, *Privacy by Design in Law, Policy and Practice*, *op. cit*., p. 10.

[63] Ann Cavoukian, *Privacy by Design in Law, Policy and Practice*, *op. cit*., p. 11.

[64] Ann Cavoukian, *Privacy by Design - The 7 Foundational Principles*, p. 2, available at https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf (last accessed on 15 June 2017).

- ✓ **Privacy embedded into the design:** privacy safeguards must be "*embedded into the design and architecture of IT systems*" and practices, and "*not bolted on as an add-on, after the fact*". Privacy protection is therefore "*integral to the system*" and a key component "*of the core functionality being delivered*"[65].
- ✓ **Positive-sum approach:** privacy protection should not be seen as a burden but as an approach that seeks "*to accommodate all legitimate interests and objectives in a positive-sum "win-win" manner*"[66].
- ✓ **End-to-end security (full lifecycle protection):** privacy protection must be ensured "*throughout the entire lifecycle of the data involved*"[67], from the start to the end of processing operations, including during data deletion (deletion that has to be ensured in a secured manner).
- ✓ **Visibility and transparency:** the implementation of privacy safeguards must be visible and transparent. All stakeholders must be assured that personal data are processed in a coherent manner to the promises made in terms of privacy preservation, "*subject to independent verification*"[68].
- ✓ **Respect for user privacy (user centric):** the reflexion on privacy safeguards to be implemented must aim to provide a high level of protection for the interest of data subjects, by offering them measures such as "*strong privacy defaults*" and "*appropriate notice*"[69].

At the level of the European Union, the concept of privacy by design and by default has been included in the new framework on data protection and will be mandatory from May 2018. This new framework essentially aims at ensuring full compliance of processing operations with the data protection law during the entire lifecycle management of personal data, by implementing appropriate technical and organisational measures to be determined having regards to the particular nature of the processing.

Indeed, the GDPR and the Directive on personal data protection for the police and criminal justice sector develop the following, in provisions dedicated to *"data protection by design and by default"*[70]:

- The controller or the processor must "*implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of* (the GDPR and the Directive) (...) *and protect the rights of data subjects*". This must be done *"taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing, as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing"*.

[65] Ann Cavoukian, *Privacy by Design - The 7 Foundational Principles*, *op. cit*. p. 2.

[66] Ann Cavoukian, *Privacy by Design - The 7 Foundational Principles*, *op. cit*. p. 2.

[67] Ann Cavoukian, *Privacy by Design - The 7 Foundational Principles*, *op. cit*. p. 2.

[68] Ann Cavoukian, *Privacy by Design - The 7 Foundational Principles*, *op. cit*. p. 2.

[69] Ann Cavoukian, *Privacy by Design - The 7 Foundational Principles*, *op. cit*. p. 2.

[70] Article 25 of the GDPR and article 20 of the Directive for the police and criminal justice sector.

- The afore-mentioned implementation of appropriate technical and organisational measures must take place "*both at the time of the determination of the means for processing and at the time of the processing itself*".
- The controller must also "*implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons".*
- The GDPR adds that compliance with the above-mentioned requirements may be demonstrated by using an "*approved certification mechanism*" as they are regulated in Article 42 of the GDPR.

Since the privacy by design principle implies to implement as soon as possible, into the design, the measures that enable to comply with the data protection legislation and to protect appropriately citizens' rights and freedoms, a full implementation of this principle implies the prior performance of a PIA, "*as early as possible in the design of the processing operations*"[71], in order to determine accurately legal requirements to be implement and risks that are likely to result from the system or the project and that must be counteracted by technical and organisational measures.

Conclusion on privacy by design:

As an essential requirement of the GDPR and of the Directive for the police and criminal justice sector, the principle of privacy by design will be implemented during the MANDOLA research, in the light of the meaning given to this concept by both Dr. Ann Cavoukian and the new EU framework on personal data protection. Consequently, the following principles will be taken into account:

- **Privacy by design is a proactive approach**, which implies that the MANDOLA consortium assess the potential impacts of both the research project and of the MANDOLA outcomes, in order to highlight potential risks and include at the earlier stage possible the privacy safeguards that are appropriate to mitigate or suppress those risks. Such an assessment may imply the performance of a privacy impact assessment.
- **Privacy by design must ensure a privacy protection by default**, which automatically applies where possible. In particular, this protection by default must include mechanisms that ensure data minimisation, time limitation and the inaccessibility of data to other persons than a definite number of individuals.
- **Privacy by design implies that privacy safeguards are embedded into the design and architecture** of the system and practices, and that they are therefore a key component of the core functionality being delivered.
- **Positive-sum approach:** privacy protection should not be seen as a burden but as an

[71] Article 29 Data Protection Working Party, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679* (WP248), 4 April 2017, p. 13, http://ec.europa.eu/newsroom/document.cfm?doc_id=44137 (last accessed on 15 June 2017).

approach that seeks to accommodate all legitimate interests, for the benefit of all relevant stakeholders.

- **Full lifecycle protection of personal data:** privacy protection must be ensured throughout the entire lifecycle management of personal data, from the start to the end of data processing operations (i. e. from the collection to the deletion of personal data). Comprehensive procedural safeguards must particularly ensure the accuracy, confidentiality, integrity, physical security and secure deletion of personal data.
- **Visibility and transparency:** the implementation of privacy safeguards must be visible and transparent.
- **Respect for user privacy (user centric):** the reflexion on privacy safeguards to be implemented must aim at providing a high level of protection for the interest of data subjects, by offering them measures such as strong privacy defaults and appropriate notice.

3.3 Sources of the proposed method

In order to assess the MANDOLA project's outcomes, a specific method has been created, based on existing methods and guidelines, which are adapted to the specificities of the project and refined in order to ensure an ethical and appropriate approach, taking into account the purpose which is the protection, to the utmost extent, of citizens' rights and freedoms.

Main sources of the proposed method are the following:

- The ePOOLICE EU project method[72];
- The French EBIOS method[73];
- ENISA guidelines on risk management[74];
- The Article 29 Data Protection Working Party Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679[75];

[72] Estelle De Marco *in* Estelle De Marco *et al.*, Deliverable D3.3 - Legal recommendations - ePOOLICE project (early Pursuit against Organized crime using envirOnmental Scanning, the Law and IntelligenCE systems), projet n° FP7-SEC-2012-312651, version 1.3 of 10 December 2014, Sections 4 and 5; Estelle De Marco *in* Estelle De Marco*,* Nasredine Semmar *et al.*, *Deliverable D3.4 - Final report*, ePOOLICE project (early Pursuit against Organized crime using envirOnmental Scanning, the Law and IntelligenCE systems), projet n° FP7-SEC-2012-312651, version 1.4 of 28 December 2015 (Doc. ID EPO-1512-WP03-004-V1.4-DV-RE), Section 4 and Annex 1. Both these deliverables are available at https://www.epoolice.eu/ (last accessed on 15 June 2017).

[73] EBIOS 2010, Expression des Besoins et Identification des Objectifs de Sécurité, ANSSI, 25 October 2011, available at https://www.ssi.gouv.fr/guide/ebios-2010-expression-des-besoins-et-identification-des-objectifs-de-securite/ (in French). See also an overview in English at https://www.ssi.gouv.fr/archive/en/confidence/documents/methods/ebiosv2-methode-plaquette-2003-09-01_en.pdf (URLs last accessed on 15 June 2017). This method has originally been developed by the French ANSSI to assess and treat risks relating to information system security, and may be adapted to assess and treat privacy risks generated by new projects. It is compliant with international norms ISO/IEC 31000, 27005, and 27001.

[74] ENISA website, Risk management, available at http://www.enisa.europa.eu/activities/risk-management (last accessed on 15 June 2017).

[75] Article 29 Data Protection Working Party, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679* (WP248), 4 April 2017, http://ec.europa.eu/newsroom/document.cfm?doc_id=44137 (last accessed on 15 June 2017).

- The method proposed by the research consortium of the PIAF (Privacy Impact Assessment Framework) EU project[76];
- Article 35 of the GDPR and article 26 of the Directive on the protection of personal data for the police and criminal justice sector[77];
- One of the first books on Privacy Impact Assessment edited by David Wright and Paul De Hert[78];
- The PIA manual published by the French Data Protection Authority's (CNIL's) in 2015, based on the EBIOS method[79];
- The method published in 2012 by the CNIL in order to manage risks for freedoms and privacy [80];
- The method proposed by the research consortium of the VIRTUOSO (Versatile InfoRmation Toolkit for end-Users oriented Open-Sources explOitation) EU project[81];
- The United Kingdom Information Commissioner's Office (ICO) PIA code of practice[82];
- The Article 29 Data Protection Working Party's opinion on the data protection impact assessment template for Smart Grid and Smart Metering Systems developed by the Expert Group 2 of the European Commission[83].

[76] Paul De Hert, Dariusz Kloza, David Wright *et al.*, *Recommendations for a privacy impact assessment framework for the European Union*, PIAF (Privacy Impact Assessment Framework) project, Grant agreement JUST/2010/FRAC/AG/1137 – 30---CE---0377117/00---70, Deliverable D3, November 2012, p.5, available at http://www.piafproject.eu/Deliverables.html (last accessed on 15 June 2017).

[77] Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (known as the "General Data Protection Regulation" or "GDPR"), http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:FULL and Directive (EU) 2016/680 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. In relation to the wording "Directive for the police and criminal justice sector", See for eample European Commission, *Reform of EU data protection rules*, http://ec.europa.eu/justice/data-protection/reform/index_en.htm (URLs last accessed on 12 May 2017).

[78] David Wright and Paul De Hert, *Privacy Impact Assessment*, Law, Governance and Technology Series volume 6, Springer, 2012, pp. 117 *et seq*.

[79] CNIL, *Privacy Impact Assessments: the CNIL publishes its PIA manual*, 10 July 2015, https://www.cnil.fr/fr/node/15798 (last accessed on 15 June 2017).

[80] CNIL, *Gérer les risques sur les libertés et la vie privée, the method*, June 2012, https://www.cnil.fr/sites/default/files/typo/document/CNIL-Guide_Securite_avance_Methode.pdf (last accessed on 15 June 2017).

[81] Gabriela Bodea, Marc van Lieshout, Linda Kool, Leo van de Wees, *D03.01.01 - A privacy impact assessment framework for the use of open source information in border control and security*, VIRTUOSO EU project (Versatile InfoRmation Toolkit for end-Users oriented Open-Sources explOitation), project number FP7-SEC-GA-2009-242352, Deliverable D3.1.1 (WP 3 - Privacy, ethical and legal aspects), 31 October 2010, available on http://www.virtuoso.eu/VIRTUOSO/servlet/document.listPublic (last accessed on 15 June 2017).

[82] ICO, *Conducting privacy impact assessments code of practice*, 2014, https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf (last accessed on 14 June 2017).

[83] the EC recommendation of 9 March 2012 on preparations for the roll-out of smart metering systems (2012/148/EU), §I, 3 (c), available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:073:0009:0022:EN:PDF (last accessed on 14 June 2017); The DPIA template has been submitted to the Article 29 Data Protection Working Party: see its Opinion 04/2013 on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems ('DPIA Template') prepared by Expert Group 2 of the Commission's Smart Grid Task Force (WP 205), adopted on 22 April 2013, p. 7, available

3.4 Steps included in existing methods and justification of choices

The analysis of all the above-mentioned works and guidelines relating to PIA and DPIA enables to identify seven main steps whose content should be included in a **PIA**, which **will be understood in our study in a broad sense, as including the assessment of risks posed by a project to the right to private life and to personal data protection, and more widely to the other rights and freedoms either exercised by individuals in their respective personal spheres, or restricted by extension because of a privacy limitation or a personal data use**[84].

These seven fundamental steps are the following[85]:

1. Determining the necessity of a PIA and its scale

An initial assessment is recommended, to determine whether a PIA is necessary, when not legally mandatory. Depending on the PIA guidelines or the legal publication tackling this issue, one or several questions have to be answered for such a determination. Most protective ones require the performance of a PIA when "*the project involves the processing of personal data or could impact any type of privacy*"[86] .

More reasonably, other methods require the performance of a PIA only where the processing is "*likely to present privacy risks*"[87] to the rights and freedoms of individuals. The new EU framework on the protection of personal data requires for its part the performance of a DPIA where processing operations, "*in particular* (where they use) (...) *new technologies,* (...) are "*likely to result in a high risk to the rights and freedoms of natural persons*", taking into account "*the nature, scope, context and purposes*" of this processing[88]. As a consequence a DPIA "*will in particular be required in case of (a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person; (b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or (c) a systematic monitoring of a publicly accessible area on a large scale*" [89]. In addition, the

at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp205_en.pdf (URLs last accessed on 14 June 2017).

[84] An example provided by the Article 29 Data Protection Working Party is the financial loss that could result from inaccurate billing or price discrimination, which may be caused by a personal data processing (Article 29 Data Protection Working Party, Opinion 04/2013 (WP205), *op. cit*., p. 7). Another example could be a (even temporary) deprivacy of liberty due to an investigation targeting someone other than the perpetrator of a penal offence, opened on the basis of the processing of non-reliable personal data.

[85] A large part of the analysis proposed in this section is based on Estelle De Marco previous works in Estelle De Marco *et al.*, Deliverable D3.3 - Legal recommendations - ePOOLICE project (early Pursuit against Organized crime using envirOnmental Scanning, the Law and IntelligenCE systems), projet n° FP7-SEC-2012-312651, version 1.3 of 10 December 2014, Section 3.2.2.1, available at https://www.epoolice.eu/ (last accessed on 15 June 2017).

[86] Paul De Hert, Dariusz Kloza, David Wright *et al.*, Recommendations for a privacy impact assessment framework for the European Union, PIAF (Privacy Impact Assessment Framework) project, Grant agreement JUST/2010/FRAC/AG/1137 – 30--CE--0377117/00--70, Deliverable D3, November 2012, p.24, available at http://www.piafproject.eu/Deliverables.html (last accessed on 15 June 2017).

[87] Paul De Hert, Dariusz Kloza, David Wright *et al.*, *Recommendations for a privacy impact assessment framework for the European Union, op. cit*. p.24.

[88] Article 35 §1 of the General Data Protection Regulation.

[89] *Ibid.,* §3.

Article 29 working party provides guidelines in order to assess whether a processing is likely to result in such a high risk[90].

Indeed, it does not seem necessary to conduct a PIA for the solely reason that personal data are processed, since it may expend privacy policy or compliance resources needlessly[91], where a strict respect of the personal data protection legislation could be enough to ensure the data subjects' protection.

Therefore, to the MANDOLA research consortium[92], the best way to determine the necessity of a PIA seems to answer the following questions:

- Is a PIA legally mandatory?
- If not, does the project present any privacy risk?[93]

If the answer of one of these questions is yes, a PIA has to be conducted.

Where a PIA seems necessary its scale must also be determined, depending of the level of risks presented by the project. Some guidelines distinguish on that issue small-scale PIA and full-scale PIA, which is more detailed, distinction that the PIAF EU project research consortium considers more or less artificial[94].

This step will be included as described above in the MANDOLA assessment method.

2. Determining the assessment team and its objectivity

Assessors must be identified, as well as the persons, within the organisation or the consortium which conducts the project to be assessed, who decide (i) to start to conduct a PIA, (ii) on the PIA terms and reference, the resources allocated to the PIA and its timeframe, (iii) to conduct the PIA, (iv) to approve the final results, and who decide (v) on the way the recommendations will be implemented[95].

[90] Article 29 Data Protection Working Party, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679* (WP248), 4 April 2017, pp. 7 *et seq*., http://ec.europa.eu/newsroom/document.cfm?doc_id=44137 (last accessed on 15 June 2017).

[91] Paul De Hert, Dariusz Kloza, David Wright *et al*., *Recommendations for a privacy impact assessment framework for the European Union*, *op. cit*., p.25.

[92] A same approach has been retained in the ePOOLICE EU project. See Estelle De Marco *in* Estelle De Marco, Nasredine Semmar *et al*., *Deliverable D3.4 - Final report*, ePOOLICE project (early Pursuit against Organized crime using envirOnmental Scanning, the Law and IntelligenCE systems), projet n° FP7-SEC-2012-312651, version 1.4 of 28 December 2015 (Doc. ID EPO-1512-WP03-004-V1.4-DV-RE), Section 4 (PIA of the ePOOLICE prototype), available at https://www.epoolice.eu/ (last accessed on 15 June 2017).

[93] This question is to be answered after having considering some "what if" scenarios, to find out what could happen if the project is implemented. According to the PIAF research consortium, to consider the question to know if a PIA is to be initiated is the "most preferable" approach from a privacy protection point of view: see Paul De Hert, Dariusz Kloza, David Wright *et al*., *Recommendations for a privacy impact assessment framework for the European Union*, *op. cit*., p.24.

[94] Paul De Hert, Dariusz Kloza, David Wright *et al*., *Recommendations for a privacy impact assessment framework for the European Union*, PIAF (Privacy Impact Assessment Framework) project, Grant agreement JUST/2010/FRAC/AG/1137 – 30--CE--0377117/00--70, Deliverable D3, November 2012, p. 26, available at http://www.piafproject.eu/Deliverables.html (last accessed on 15 June 2017).

[95] Paul De Hert, Dariusz Kloza, David Wright *et al*., *Recommendations for a privacy impact assessment framework for the European Union, op. cit*., pp.26-27.

The new EU General Data Protection Regulation (GDPR) and the new Directive on personal data protection for the police and criminal justice sector respectively requires or enables the involvement of the data protection officer, when such an officer has been designated[96].

The EBIOS method also includes in this step, which is in the latter method a sub-step of another step that aims at describing the framework of the study[97], the possibility to specify the selection criteria of these persons, internal and external communication mechanisms, and decision-making process to be pursued[98].

Assessors must moreover "*act with professional independence*", since a PIA needs to be "*an honest investigation*". Therefore, assessors must be independent from the others persons working on the project or the persons responsible for the project to be assessed, they must have the necessary expertise, resources and time to conduct the PIA, and they must do their best efforts to recognise their potential subjectivity and must both declare it in the report and justify each of the positions they take[99].

Most of the above-mentioned requirements have been included in this step of the ePOOLICE EU project PIA[100].

This step will be included in the MANDOLA assessment method, and will closely follow the content that has been proposed in the ePOOLICE project, with thin modifications taking into account the GDPR requirements.

3. Description of the scope and framework of the study

The content of this step differs somewhat depending on the guidelines to which it is referred. Risk management guidelines such as ENISA guidelines[101] and the French EBIOS method[102] (guidelines which target all kind of risks an organisation may face, and not

[96] Article 35 of the GDPR; article 27 and 34 (c) of the new Police Directive.

[97] See the following step n°3.

[98] EBIOS 2010, Expression des Besoins et Identification des Objectifs de Sécurité, ANSSI, 25 October 2011, guide methodologique (methodological guide), https://www.ssi.gouv.fr/guide/ebios-2010-expression-des-besoins-et-identification-des-objectifs-de-securite/ and more precisely https://www.ssi.gouv.fr/uploads/2011/10/EBIOS-1-GuideMethodologique-2010-01-25.pdf (URLs last accessed on 15 June 2017).

[99] See (including for all quotations in this paragraph) Paul De Hert, Dariusz Kloza, David Wright *et al.*, *Recommendations for a privacy impact assessment framework for the European Union, op. cit.*, p. 23. In the same sense, see Article 29 Data Protection Working Party, Opinion 04/2013 on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems ('DPIA Template') prepared by Expert Group 2 of the Commission's Smart Grid Task Force (WP 205), adopted on 22 April 2013, p. 13, available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp205_en.pdf (last accessed on 14 June 2017).

[100] Estelle De Marco in *Estelle De Marco,* Nasredine Semmar *et al.*, *Deliverable D3.4 - Final report*, ePOOLICE project (early Pursuit against Organized crime using envirOnmental Scanning, the Law and IntelligenCE systems), projet n° FP7-SEC-2012-312651, version 1.4 of 28 December 2015 (Doc. ID EPO-1512-WP03-004-V1.4-DV-RE), Section 4 and Annex 1, available at https://www.epoolice.eu/ (last accessed on 15 June 2017).

[101] ENISA guidelines on Risk Management, available on the ENISA website at http://www.enisa.europa.eu/activities/risk-management (last accessed on 15 June 2017).

[102] EBIOS 2010, Expression des Besoins et Identification des Objectifs de Sécurité, ANSSI, 25 October 2011, available at https://www.ssi.gouv.fr/guide/ebios-2010-expression-des-besoins-et-identification-des-objectifs-de-securite/ (in French). See also an overview in English at https://www.ssi.gouv.fr/archive/en/confidence/documents/methods/ebiosv2-methode-plaquette-2003-09-01_en.pdf (URLs last accessed on 15 June 2017).

specifically risks on privacy or fundamental freedoms generated by a particular project[103]) differ on the classification of the precise sub-steps to follow in order to achieve this general task, but give to the latter the same elements of content: both suggest to describe the framework of the study (aim of the study, expected deliverables, working structure…); its environment (description of the external and internal environment, including the definition of risks in this context and the chosen team to conduct the study); its scope and boundaries (description of the project to be assessed including its duration, goals and objectives, identification of the aim and approach chosen for the assessment, roles and responsibilities, dependencies with other projects …); the parameters to be taken into account (including constraints and legal requirements); and the origin of threats. They also both advise to identify here all the "*basic parameters within which risks must be managed*"[104], namely the assets to be protected (primary assets), the resources that support them (supporting assets), the existing security measures, and the metrics that are retained in order to manage risks (security criteria, severity and probability scale, and risk management criteria)[105].

Guidelines dedicated to PIA or DPIA generally call this step "*project description*"[106] or "*description of processing operations*"[107], and tend to include in it the same elements as the ones studied above, even if they are sometimes less specific and at the exception of some analyses that these methods already include as part of other steps (for example, the parameters to be taken into account are generally discussed within the framework of the step dedicated to risk assessment, which we will analyse below).

The research consortium of the PIAF project notably advises, in this step, to describe the project in such a manner as to permit a "*comprehensive identification and management of privacy risks*"[108], which means to provide a "*general description of the project*" and "*a mapping of information flows*[109] *and/or an analysis of its impact on other privacy types*". Firstly, the general description of the project should include a description of the context and of the motivations underlying the project, a statement of the objectives, a description of the PIA process and of the persons involved, an outline of first-order impacts and second-order

[103] The French Data Protection Authority (CNIL) has published a PIA manual based on the EBIOS method: see CNIL, *Privacy Impact Assessments: the CNIL publishes its PIA manual*, 10 July 2015, https://www.cnil.fr/fr/node/15798 (last accessed on 15 June 2017).

[104] ENISA website, Risk Management, "Definition of scope and framework", available at http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/rm-process/crm-strategy/scope-framework (home/our activities/risk management/current risk/ rm inventory/rm process/crm strategy/Scope & Framework), last accessed on 15 June 2017.

[105] On this paragraph see ENISA, "Definition of scope and framework", above mentioned; EBIOS 2010, Méthode de gestion des risques, op. cit., methodological guide p. 11 and p. 34 *et seq*.

[106] Paul De Hert, Dariusz Kloza, David Wright *et al.*, *Recommendations for a privacy impact assessment framework for the European Union*, PIAF (Privacy Impact Assessment Framework) project, Grant agreement JUST/2010/FRAC/AG/1137 – 30--CE--0377117/00--70, Deliverable D3, November 2012, p.27, available at http://www.piafproject.eu/Deliverables.html (last accessed on 15 June 2017).

[107] See for instance the EC recommendation of 9 March 2012 on preparations for the roll-out of smart metering systems (2012/148/EU), §I, 4, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:073:0009:0022:EN:PDF (last accessed on 14 June 2017).

[108] Paul De Hert, Dariusz Kloza, David Wright *et al.*, *Recommendations for a privacy impact assessment framework for the European Union, op. cit*., p.27.

[109] The mapping of information flows is also part of the ICO Conducting privacy impact assessments code of practice, 2014, https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf (last accessed on 14 June 2017).

implications, an outline cost/benefit analysis, a description of roles, responsibilities and organisational privacy management structure and policy, a description of the way the project could affect end-users, in addition to the description of the "*initial conceptual design of the scheme*", a brief description of options and sub-options and important milestones. Secondly, the mapping of information flows sub-step aims at describing personal data processing, measures taken to respect legal requirements in that field, and other privacy implications if any[110].

In a more limited extent, the French Data Protection authority's (CNIL) guide which aim at applying the EBIOS method to personal data processing to assess privacy risks[111] reduces this step to the description of the "*processing(s) of personal data under consideration, its (their) purposes and stakes*", to the identification of the "*data controller and the processors*", and to the definition and description in details of (1) "*the personal data concerned, their recipient and retention periods*" and (2) "*the processes and personal data supporting assets for the entire personal data life cycle (from collection to erasure)*". To be recalled that the scope of this assessment method is very reduced since it is restricted to the risks that might threaten the personal data that are processed, without having regards to the risks posed to other fundamental rights as assets or to the risks posed by the whole system beyond what strictly relates to personal data processing operations.

The importance of conducting the PIA taking into account the specificities of the sector within which the project will be implemented (which implies to describe this project and its context) is also stressed by the Article 29 Data Protection Working Party, since such an approach enables the identification of specific risks and of corrective measures matching those risks[112].

In addition, the new EU GDPR and Directive on personal data protection for the police and criminal justice sector require at least a "*description of the envisaged processing operations"* (which must be "general" in the Directive and "systematic" in the GDPR), and "*safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation* (or Directive) *taking into account the rights and legitimate interests of data subjects and other persons concerne*d", classifying those safeguards, security measures and mechanisms in the category of "*measures envisaged to address the risks"*[113].This last requirement is in line with risk management methods, at the exception that, in the latter methods, security measures (and contingently, in our opinion, measures aiming at complying with legal requirements, if these are included in the assets) are supposed to be presented in the current step relating to context description whereas risk management measures are the subject of the step that follows the risk assessment step (see step number 6 below).

[110] Paul De Hert, Dariusz Kloza, David Wright *et al.*, *Recommendations for a privacy impact assessment framework for the European Union, op. cit.*, p. 28.

[111] Cnil, *Privacy Impact Assessments: the CNIL publishes its PIA manual*, 10 July 2015, PIA Manual 1 - Methodology, p. 11, https://www.cnil.fr/fr/node/15798 and more exactly https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-1-Methodology.pdf (last accessed on 15 June 2017).

[112] Article 29 Data Protection Working Party, Opinion 04/2013 on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems ('DPIA Template') prepared by Expert Group 2 of the Commission's Smart Grid Task Force (WP 205), adopted on 22 April 2013, p. 8, available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp205_en.pdf (last accessed on 14 June 2017).

[113] Article 35, 7 of the GDPR and article 27, 2 of the Police Directive.

The GDPR adds the necessity to include in a DPIA *"a systematic description of* (...) *the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller*", and "*an assessment of the necessity and proportionnality of the processing operations in relation to the purposes"*[114].

These two last requirements form part of the description of the envisaged processing operations in the light of all data protection requirements on the one hand and of ECHR requirements on the other hand. They are in line with the outcomes of our analysis of the legal context[115], and support the need for assessing the project in the light of both the data protection legislation and the ECHR.

Taking inspiration of all the above-mentioned methods, the ePOOLICE EU project includes in this step the content proposed by risk management methods[116] (at the exception of certain elements of contents, studied in other steps of the assessment, such as the working structure which is analysed in the second step of the method relating to the assessment team) and more particularly the eBIOS method, adapting the latter to the needs implied by the performance of a PIA, by taking into consideration PIA and DPIA recommendations, and the new EU framework for personal data protection. This has especially led to the description of the project in the light of legal requirements, including the personal data protection legislation and the ECHR requirements, and to the consideration, as part of the context, of the potential difficulties that the project's features and known end-user expectations may pose in relation to personal data and privacy protection.

The content of this step will be included in the MANDOLA assessment method, and will correspond to the one proposed in the ePOOLICE project, slightly modified in order to enhance the efficiency of the assessment. For example, assets will be studied before risk management criteria, and assets will include both (1) the legal requirements that must be respected based on the ECHR and the Data Protection Law and studied in the MANDOLA deliverable D2.2[117], and (2) other citizens fundamental rights. As a consequence, existing security measures will be studied together with existing safegards aiming to ensure legal compliance.

4. Stakeholders consultation

According to several methods including the PIAF method and the ePOOLICE method, the project needs to be submitted to all relevant stakeholders to gather their views, which need to be taken into consideration. According to the research consortium of the PIAF EU project,

[114] Article 35, 7 of the GDPR.

[115] Estelle De Marco *et al.*, MANDOLA deliverable D2.2 - *Identification and analysis of the legal and ethical framework*, MANDOLA project (Monitoring ANd Detecting OnLine hAte speech) - GA noJUST/2014/RRAC/AG/HATE/6652, http://mandola-project.eu/, 12 July 2017.

[116] Estelle De Marco in *Estelle De Marco,* Nasredine Semmar *et al.*, *Deliverable D3.4 - Final report*, ePOOLICE project (early Pursuit against Organized crime using envirOnmental Scanning, the Law and IntelligenCE systems), projet n° FP7-SEC-2012-312651, version 1.4 of 28 December 2015 (Doc. ID EPO-1512-WP03-004-V1.4-DV-RE), Section 4 and Annex 1, available at https://www.epoolice.eu/ (last accessed on 15 June 2017).

[117] Estelle De Marco *et al.*, MANDOLA deliverable D2.2 - *Identification and analysis of the legal and ethical framework, op. cit.*

the objective is to achieve a "'*win-win' result so that everyone benefit*"[118]. This notion of "win-win" result recalls the spirit of the privacy by design approach[119].

Less ambitious, the new GDPR requires that "*where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations*"[120].

The research consortium of the MANDOLA project will implement the content of this step as it is described in the PIAF EU method and in the ePOOLICE method, in a specific step to be followed after the first identification of the risk treatment measures.

5. Assessment of the risks to rights and freedoms

Risk assessment is considered by some studies and guidelines as a sub-step of a "risk management" step, along with risk treatment[121] (which is also called risk mitigation[122]) and residual risks acceptance (which is an optional sub-step according to the ENISA and EBIOS guidelines related to risk management).

The new GDPR and the new Directive on personal data protection for the police and criminal justice sector both require to include in a DPIA such "*an assessment of the risks to the rights and freedoms of data subjects (...)*"[123].

This step aims at identifying risks caused to fundamental rights, taking into account all the elements of the project (features, context, uses…). Impacts include "*physical, material or non-material damages*" due to "*discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage*" according to the new EU GDPR[124], in the light of the project description and the notion of protected rights.

[118] Paul De Hert, Dariusz Kloza, David Wright *et al.*, Recommendations for a privacy impact assessment framework for the European Union, PIAF (Privacy Impact Assessment Framework) project, Grant agreement JUST/2010/FRAC/AG/1137 – 30--CE--0377117/00--70, Deliverable D3, November 2012, p. 29, available at http://www.piafproject.eu/Deliverables.html (last accessed on 15 June 2017).

[119] See above our section dedicated to Privacy by design.

[120] Article 35, 9 of the GDPR.

[121] In that sense see notably the ENISA guidelines on Risk Management, available on the ENISA website at http://www.enisa.europa.eu/activities/risk-management (last accessed on 14 June 2017); EBIOS 2010, Méthode de gestion des risques, 25 January 2010, p. 11, available at https://www.ssi.gouv.fr/guide/ebios-2010-expression-des-besoins-et-identification-des-objectifs-de-securite/ (last accessed on 15 June 2017).

[122] In that sense see notably Paul De Hert, Dariusz Kloza, David Wright *et al.*, *Recommendations for a privacy impact assessment framework for the European Union*, *op. cit.*, p.30; Gabriela Bodea, Marc van Lieshout, Linda Kool, Leo van de Wees, *D03.01.01 - A privacy impact assessment framework for the use of open source information in border control and security*, VIRTUOSO EU project (Versatile InfoRmation Toolkit for end-Users oriented Open-Sources explOitation), project number FP7-SEC-GA-2009-242352, Deliverable D3.1.1 (WP 3 - Privacy, ethical and legal aspects), 31 October 2010, available on http://www.virtuoso.eu/VIRTUOSO/servlet/document.listPublic (last accessed on 15 June 2017).

[123] Article 35, 7 of the GDPR and article 27, 2 of the Police Directive.

[124] Recital n°75 of the GDPR.

As regard the definition of risks, each of them may be defined as composed of a threat, a source of threat, a vulnerability and an impact[125], following the terminology used by the French EBIOS method, which is compliant with several international norms[126]. This means that the identification of risks implies following different sub-steps to identify feared events, threats and their sources (if not identified in the previous step), and vulnerabilities, knowing that the combination of a threat, of a threat origin and of a vulnerability gives a "*threat scenario*", according to the EBIOS method. The determination of the severity (or gravity) of a feared event (in other word the importance of the impact of the event if it occurs) and of the probability (or opportunity / likehood) that threat scenarios occur, further allows giving to identified risks a level of severity[127].

The Article 29 Data Protection Working Party stresses the importance to give "*enough details and specific guidance on the concept of vulnerability*" and on "*how to calculate and prioritise risks*"[128]. More specifically on the determination of impacts, the Article 29 Data Protection Working Party highlights the necessity, in the context of a risk driven approach, to "*directly address the actual impacts on the data subjects*", even second-order implications. According to the working party, it is "*impossible to correctly identify and implement the necessary controls and safeguards*" if "*the risks and their impact (…) are not considered in their entirety*"[129].

According to ENISA guidelines, it is moreover really important, within the framework of that step, to identify and record all the risks posed by the project, including those that are already controlled by the entity responsible for the project[130]. For this reason, ENISA guidelines advise to perform this assessment without taking into acccount existing measures

[125] EBIOS 2010, Méthode de gestion des risques, 25 January 2010, op. cit., p. 11. The ENISA guidelines on Risk assessment propose a similar approach: a risk is defined as "*the potential that a given threat will exploit vulnerabilities of an asset (…) and therefore cause harm to the organisation*" (ENISA website, home/our activities/risk management/current risk/ rm inventory/Glossary, available at http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/glossary - last accessed on 15 June 2017). ENISA guidelines add that "*in general, a risk can be related or characterized*" by its origin; a certain activity, event or incident (i.e. threat); its consequences; a specific reason for its occurrence, protective mechanisms and controls; time and place of occurrence (ENISA website, home/our activities/risk management/current risk/ rm inventory/rm process/Risk Assessment, available at http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/rm-process/risk-assessment - last accessed on 15 June 2017). The ENISA definition of risks is also the definition proposed by the norm ISO/IEC 27005:2008.

[126] Norms ISO/IEC 31000, 27005, and 27001. See EBIOS 2010, Expression des Besoins et Identification des Objectifs de Sécurité, ANSSI, 25 October 2011, presentation webpage, available at https://www.ssi.gouv.fr/guide/ebios-2010-expression-des-besoins-et-identification-des-objectifs-de-securite/ (last accessed on 15 June 2017).

[127] According to the EBIOS method. PIA guidelines do not always use the same terminology but propose similar content to the risk assessment phase: see notably Paul De Hert, Dariusz Kloza, David Wright *et al.*, *Recommendations for a privacy impact assessment framework for the European Union,* PIAF (Privacy Impact Assessment Framework) project, Grant agreement JUST/2010/FRAC/AG/1137 – 30---CE---0377117/00---70, Deliverable D3, November 2012, p.30, available at http://www.piafproject.eu/Deliverables.html (last accessed on 15 June 2017).

[128] Article 29 Data Protection Working Party, Opinion 04/2013 on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems ('DPIA Template') prepared by Expert Group 2 of the Commission's Smart Grid Task Force (WP 205), adopted on 22 April 2013, p. 8, available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp205_en.pdf (last accessed on 14 June 2017).

[129] Article 29 Data Protection Working Party, Opinion 04/2013 on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems, *op. cit*. p. 7.

[130] ENISA guidelines on Risk Management, *op. cit*.

that aim to control the feared events[131]. However, such measures may be appropriate to counteract a specific feared event or a specific impact. In addition, some measures implemented to ensure compliance with legal requirements (the latter forming part, ideally, of primary assets) may already be appropriate to counteract the severity or the likelihood of the feared event. For these reasons, the ePOOLICE method[132] has rather followed the CNIL's advice to assess in this step the severity of the impact both without having regards and taking into account the existing measures already implemented or that are planned to be implemented[133].

According to the EBIOS method, existing measures may have the effect of protecting the security needs of primary assets (these measures are mainly prevention and recovery measures), of reducing identified impacts (prediction and preparation, prevention, containment, fight, recovery, restoration, compensation…), of counteracting each identified threat source (prediction and preparation, deterrence, detection, containment…), of ensuring protection against threats (these measures are mainly detection and protection measures), and of reducing supporting assets' vulnerabilities (these measures are mainly prevention and protection measures)[134].

As regard the method to be followed in order to carry out the identification of the components of risks (threats, sources of threat, vulnerabilities and an impacts), some techniques are proposed, as team-based brainstorming, or structured techniques such as flow-charting or Hazard and Operability studies[135].

To methodogically identify and classify risks and their components, the EBIOS method proposes a set of templates to fill in[136]. The French Data Protection Authority (CNIL) also proposes templates that may be used to assess the impact on privacy of personal data processing (the scope of the assessment being reduced to the threats to personal data that are processed, as already analysed), derived from the EBIOS method[137]. The research consortium of the VIRTUOSO EU project[138] has also created a set of templates to make the

[131] See for example ENISA guidelines on Risk Management, *op. cit.*

[132] Estelle De Marco in *Estelle De Marco,* Nasredine Semmar *et al.*, *Deliverable D3.4 - Final report*, ePOOLICE project (early Pursuit against Organized crime using envirOnmental Scanning, the Law and IntelligenCE systems), projet n° FP7-SEC-2012-312651, version 1.4 of 28 December 2015 (Doc. ID EPO-1512-WP03-004-V1.4-DV-RE), Section 4 and Annex 1, available at https://www.epoolice.eu/ (last accessed on 15 June 2017).

[133] Cnil, *Privacy Impact Assessments: the CNIL publishes its PIA manual*, 10 July 2015, PIA Manual 1 - Methodology, https://www.cnil.fr/fr/node/15798 and more exactly https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-1-Methodology.pdf (last accessed on 15 June 2017).

[134] EBIOS 2010, Expression des Besoins et Identification des Objectifs de Sécurité, *op. cit.,* Methodological guide p. 46.

[135] ENISA guidelines on Risk Management, *op. cit*.

[136] EBIOS 2010, Expression des Besoins et Identification des Objectifs de Sécurité, *op. cit.,*

[137] Cnil, *Privacy Impact Assessments: the CNIL publishes its PIA manual*, 10 July 2015, PIA Manual 1 - Methodology, https://www.cnil.fr/fr/node/15798 and more exactly https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-1-Methodology.pdf (last accessed on 15 June 2017).

[138] EBIOS 2010, Expression des Besoins et Identification des Objectifs de Sécurité, *op. cit*.; Gabriela Bodea, Marc van Lieshout, Linda Kool, Leo van de Wees, *D03.01.01 - A privacy impact assessment framework for the use of open source information in border control and security*, VIRTUOSO EU project (Versatile InfoRmation Toolkit for end-Users oriented Open-Sources explOitation), project number FP7-SEC-GA-2009-242352, Deliverable D3.1.1 (WP 3 - Privacy, ethical and legal aspects), 31 October 2010, available on http://www.virtuoso.eu/VIRTUOSO/servlet/document.listPublic (last accessed on 8 November 2013).

PIA of its own project. These latter templates, which are close to the EBIOS ones and which follow a large part of the ENISA guidelines, may also offer inspiration for the creation of other projects' assessment method.

For its part, the ePOOLICE EU project[139] also created some templates for the purpose of the PIA performed by the research consortium, which can be a more recent and comprehensive source of inspiration in addition to this latter PIA itself, since they are based - as well as the ePOOLICE method - on the EBIOS method adapted by taking inspiration from the Article 29 Data Protection Working Party and from the works of the French Data Protection Authority (CNIL) and of the VIRTUOSO research consortium, where relevant. The method created by the ePOOLICE project will therefore be the main source of inspiration of the MANDOLA method.

This step will naturally be included in the MANDOLA assessment method. As discussed, the method developed during the ePOOLICE EU project will be largely re-used, with some adaptations that appear conducive to enhancing its efficiency (especially due to adaptations made in previous steps of the assessment). Indeed, this method appears to be one of the more comprehensive one and has received an outstanding evaluation from the European Commission in 2016[140].

In particular and as it has been highlighted in the latter project, the gathering of stakeholders' opinions will be particularly helpful to enhance the quality and relevance of the risk assessment[141] so the question of whether these stakeholders have in mind other risks for freedoms than the ones that the MANDOLA research consortium has identified will be asked during the course of the step dedicated to this collection of views.

6. Risk treatment

According to risk management methods, this step aims at choosing the risks treatment options (avoidance, optimising, retaining, transferring or sharing), taking into account the risk evaluation. It also aims at analysing residual risks, at identifying the means that need to be put in place to treat risks, at formally[142] validating the choices that are made, the security measures to implement (if not already implemented), and the persons responsible for their

[139] Estelle De Marco in *Estelle De Marco,* Nasredine Semmar *et al.*, *Deliverable D3.4 - Final report*, *op. cit*., Section 4 and Annex 1.

[140] European Commission, Research and Innovation DG, Human resources and mobility, Review report, Project n°312651, Project acronym: ePOOLICE, submitted on 27 January 2016.

[141] Paul De Hert, Dariusz Kloza, David Wright *et al.*, *Recommendations for a privacy impact assessment framework for the European Union,* PIAF (Privacy Impact Assessment Framework) project, Grant agreement JUST/2010/FRAC/AG/1137 – 30---CE---0377117/00---70, Deliverable D3, November 2012, p. 30, available at http://www.piafproject.eu/Deliverables.html (last accessed on 15 June 2017); Estelle De Marco in *Estelle De Marco,* Nasredine Semmar *et al.*, *Deliverable D3.4 - Final report*, *op. cit.*

[142] According to the EBIOS method, the organisation must formally validate the conclusions of the study, and decide if the assessed system or project is ready for operations, potentially with residual risks accepted and managed (EBIOS 2010, *op. cit*., p. 81). ENISA guidelines evoke the necessity of an approval of the action plan by the organisation's executive management, initially and throughout the entire life-cycle of the project, the executive management being kept informed through comprehensive and regular reporting (ENISA, "Risk treatment", *op. cit*.). PIA and DPIA guidelines allow here the organisation to take position on each recommendation and to not accept some of them, explaining the reasons why (Paul De Hert, Dariusz Kloza, David Wright *et al*., *op. cit*., p.32).

implementation, and at planning and following the measures implementation[143]. PIA and DPIA guidelines, which call generally this step "*risk mitigation*"[144], are along the same line. These latter guidelines moreover stress that recommendations must be detailed (in addition to identifying to whom they are directed) and that all the choices made during this step need to be justified, notably as regards the options that are retained to manage risks and the potential acceptance of some risks[145].

For their part, the new EU GDPR the new Directive on personal data protection for the police and criminal justice sector both require to include in a DPIA a description of "*the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation* (or Directive) *taking into account the rights and legitimate interests of data subjects and other persons concern*ed"[146]. In the same line, but as a subsequent step, PIA and DPIA guidelines add, generally, a "*legal compliance check*", aiming at ensuring that the project complies with privacy and data protection legal and regulatory requirements, taking into account standards, jurisprudence and the opinion of legitimate authorities like the Article 29 Data Protection Working Party ones[147].

The measures to implement to limit or eliminate risks may be of different natures (technical, operational…), may be classified in different lines of defense (preventive, protective, recuperative), may have to be implemented on different supporting assets (internal network, premises, office organisation…)[148], and may target different risks components (primary assets, potential impact, threat source, supporting assets)[149].

The method proposed by the ePOOLICE EU project[150] takes over the recommendations of the EBIOS method and of PIA guidelines as a complement, with the exception of the legal

[143] EBIOS 2010, Expression des Besoins et Identification des Objectifs de Sécurité, *op. cit*. p. 78; ENISA website, Risk Management, "Risk treatment", available at http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/rm-process/risk-treatment (home/our activities/risk management/current risk/ rm inventory/rm process/Risk Treatment), last accessed on 15 June 2017.

[144] See for instance Paul De Hert, Dariusz Kloza, David Wright *et al.*, *Recommendations for a privacy impact assessment framework for the European Union*, *op. cit.* p. 24.

[145] Paul De Hert, Dariusz Kloza, David Wright *et al.*, *Recommendations for a privacy impact assessment framework for the European Union, op. cit*., p.31; Cnil, *Privacy Impact Assessments: the CNIL publishes its PIA manual*, 10 July 2015, PIA Manual 1 - Methodology, p. 16, https://www.cnil.fr/fr/node/15798 and more exactly https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-1-Methodology.pdf. The Article 29 Data Protection Working Party also stresses the importance to give "*enough details and specific guidance"* on how to "*choose the appropriate controls and assess the residual risks that remain after the control have been put in place*": Article 29 Data Protection Working Party, Opinion 04/2013 on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems ('DPIA Template') prepared by Expert Group 2 of the Commission's Smart Grid Task Force (WP 205), adopted on 22 April 2013, p. 8, available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp205_en.pdf (URLs last accessed on 15 June 2017)

[146] Article 35, 7 of the GDPR and article 27, 2 of the Police Directive.

[147] See Paul De Hert, Dariusz Kloza, David Wright *et al.*, *Recommendations for a privacy impact assessment framework for the European Union*, *op. cit*., p.31.

[148] On all the beginning of this paragraph see for example EBIOS 2010, Expression des Besoins et Identification des Objectifs de Sécurité, *op. cit*., p 72.

[149] CNIL, *Privacy Impact Assessments: the CNIL publishes its PIA manual*, 10 July 2015, PIA Manual 1 - Methodology, *op. cit.* pp. 11 ; 14 *et seq.* ; EBIOS 2010, Expression des Besoins et Identification des Objectifs de Sécurité, *op. cit.,* p. 73.

[150] Estelle De Marco in *Estelle De Marco,* Nasredine Semmar *et al.*, *Deliverable D3.4 - Final report*, ePOOLICE project (early Pursuit against Organized crime using envirOnmental Scanning, the Law and IntelligenCE systems), projet n° FP7-SEC-2012-

compliance check which is performed during the second step of the method relating to the definition of the scope and framework of the study. This exception is justified by the fact that legal compliance is a pre-requisite to process personal data, and that the analysis of the risks to rights and freedoms must take into account the specific safeguards already implemented or whose implementation is planned to ensure compliance with law, as well as - from the point of view of the MANDOLA research - the legal requirements as assets to be protected. As regards safeguards and security measures and mechanisms designed to ensure the protection of personal data and to demonstrate compliance with law, they have been handled in a sub-step of this same step 3, as already explain previously at the occasion of the analysis of the third step relating to the description of the scope and framework of the study; however, this does not prevent the possibility to summarise them again at the occasion of the step relating to risk treatment.

The risk treatment step will naturally be included in the MANDOLA assessment method such as it has been defined by the ePOOLICE method, for the same reasons as exposed in relation with the previous step, keeping in mind that the "legal compliance check" sub-step will be included in the step relating to the definition of the scope and framework of the study, as well as the description of safeguards and security measures and mechanisms designed to ensure the protection of personal data and to demonstrate compliance with law.

7. Monitoring and review

PIA guidelines stress that the final report should be subjected to an external audit or review. They add that "*the implementation of the recommendations should be monitored*" and that the PIA should be revisited each time a modification is brought to the assessed project[151]. The ENISA guidelines are on the same line, highlighting the importance of ensuring that the project assessment remains "*relevant and updated*"[152].

In the same way, the new EU GDPR states that “*where necessary, the controller shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations*”[153]. The Article 29 data protection working party clarifies that “*risks can change as a result of change to one of the components of the processing operation (data, supporting assets, risk sources, potential impacts, threats, etc.) or because the context of the processing evolves (purpose, functionalities, etc.). Data processing systems can evolve quickly and new vulnerabilities can arise. Therefore it should be noted that the revision of a DPIA is not only useful for continuous improvement, but also critical to maintain the level of data protection*

312651, version 1.4 of 28 December 2015 (Doc. ID EPO-1512-WP03-004-V1.4-DV-RE), Section 4 and Annex 1, available at https://www.epoolice.eu/ (last accessed on 15 June 2017).

[151] Paul De Hert, Dariusz Kloza, David Wright *et al.*, Recommendations for a privacy impact assessment framework for the European Union, *op. cit.*, p.32.

[152] ENISA website, Risk management, "Monitor and review", (home/our activities/risk management/current risk/ rm inventory/rm process/Monitor & Review), available at http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/rm-process/monitor-review - last accessed on 15 June 2017).

[153] Article 35, 11 of the GDPR.

in a changing environment over longer time"[154]. The working party adds that a "*DPIA may also become necessary because the organisational or societal context for the processing activity has changed, for example because the effects of certain automated decisions have become more significant, new categories of natural persons become vulnerable to discrimination or the data is intended to be transferred to data recipients located in a country which has left the EU"*[155].

The Article 29 data protection working party further considers that "*as a matter of good practice, a DPIA should be continuously carried out on existing processing activities*" [156], and should at least "*re-assessed after 3 years, perhaps sooner, depending on the nature of the processing and the rate of change in the processing operation and general circumstances*" [157]. The working party recommends in addition to perform a PIA "*for data processing which have taken place before May 2018 and where therefore not subject to a DPIA, to make sure that 3 years after this date or sooner, depending on the context, the risks for the rights and freedoms are still mitigated*" [158].

Finally, several guidelines including those of the Article 29 data protection working party[159] recommend the publication of the assessment, in part or in full, since this helps "*foster trust in the controller's processing operations, and demonstrate accountability and transparency"*[160]. The working party emphasises that publication is "*particularly good practice* (...) *where members of the public are affected by the processing operation"*[161], especially where they are performed by public authorities.

This step will be included in the MANDOLA assessment method.

[154] Article 29 Data Protection Working Party, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679* (WP248), 4 April 2017, p. 12, http://ec.europa.eu/newsroom/document.cfm?doc_id=44137 (last accessed on 15 June 2017).

[155] *Ibid.*

[156] *Ibid.*

[157] *Ibid.*

[158] *Ibid.*

[159] For example the ICO Conducting privacy impact assessments code of practice, 2014, https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf (last accessed on 14 June 2017).

[160] Article 29 Data Protection Working Party, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679* (WP248), *op.cit.* p.17.

[161] *Ibid.*

4 Proposed PIA method

In the proposed method, the notion of PIA is understood in a broad sense in order to ensure an integral ethical approach, as including the assessment of risks posed by a project to the right to private life and to personal data protection, and more widely to the other rights and freedoms either exercised by individuals in their respective personal spheres, or restricted by extension because of a privacy limitation or a personal data use[162].

This methodology, divided into seven steps, is designed (1) to initiate the assessment "*as early as possible in the design of the processing operations*"[163], a need that has been recalled recently by the Article 29 data protection working party, and (2) to enable to modify the findings of previous steps in the course of the assessment itself. Indeed a PIA is an iterative process, which means that each step should be (and has been, during the MANDOLA project) revisited and potentially "reworked" both during the course of the development of the project and during the course of the assessment. Firstly, this ensures privacy by design and by default, which is another requirement of the GDPR and the Directive on the protection of personal data in the justice and police sectors[164], by starting the PIA during the development of the project, "*even if some of the processing operations are still unknown*"[165]. Secondly, this enables to take into account, in the results of the first steps of the assessment, some elements (such as assets or supporting assets) that are only discovered during the performance of subsequent steps, and that might have consequences on the final results.

Some steps or sub-steps of this method may not receive precise answers, during the course of the assessment of the outcomes of the MANDOLA project, since the MANDOLA consortium does not control all the elements relating to the organisations that will use these outcomes. However, the research concortium tried to follow this method as close as possible, in order to ensure that the results of the assessment reflect the final project outcome's potential impacts in the best possible way.

4.1 Determining the necessity of a PIA and its scale

In this phase, an initial assessment determines whether a PIA is necessary. In order to answer this question, two questions need to be answered:

- Is a PIA legally mandatory?

[162] An example provided by the Article 29 Data Protection Working Party is the financial loss that could result from inaccurate billing or price discrimination, which may be caused by a personal data processing (Article 29 Data Protection Working Party, Opinion 04/2013, *op. cit.*, p. 7). Another example could be a (even temporary) deprivacy of liberty due to an investigation targeting someone other than the perpetrator of a penal offence, opened on the basis of the processing of non-reliable personal data.

[163] Article 29 Data Protection Working Party, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679* (WP248), *op. cit.* p.13.

[164] Article 25 of the GDPR and article 20 of the Directive for the police and criminal justice sector.

[165] Article 29 Data Protection Working Party, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679* (WP248), *op. cit.* p.13.

- Does the project presents any privacy risks? In order to answer this last question the guidelines provided by the Article 29 working party may be of help[166].

A positive answer brought to one of these questions validates or not the necessity to conduct a PIA.

As a second step, the assessment team needs to determine if a small-scale PIA is enough, or if a full-scale PIA, more detailed, is needed, in the light of the significance of privacy risks.

4.2 Determining the assessment team and its objectivity

This step aims primarily at determining the persons involved in the PIA.

Must be identified:

- The persons who will perform the PIA (assessors), and
- The persons who decide (i) to start to conduct a PIA, (ii) on the PIA terms and reference, the resources allocated to the PIA and its timeframe, (iii) to conduct the PIA, (iv) to approve the final results, and who decide (v) on the way the recommendations will be implemented[167].
- The persons who will contribute to the study and how their input will be gathered. Where a data protection officer does exist, he or her must particularly be consulted.

The selection criteria of these persons should also be mentioned, as well as internal and external communication mechanisms, and decision-making process to be pursued.

Assessors must "*act with professional independence*", since a PIA needs to be "*an honest investigation*"[168]. Therefore, assessors must be independent. As it has been recalled, *inter alia*, in the PIAF method and in the ePOOLICE method, these assessors must have the necessary expertise, resources and time to conduct the PIA, and they must do their best efforts to recognise their potential subjectivity and must both declare it in the report and justify each of the positions they take.

Ideally, these experts should be independant from the organisation or the consortium that needs to perfom the PIA, or the PIA should be performed under the supervision of such external independent experts. Indeed, it is very difficult for any person belonging to an organisation or a community of interest to remain totally objective, even if this person is granted with a professional independence.

[166] *Ibid.* pp. 7 *et seq*.

[167] Paul De Hert, Dariusz Kloza, David Wright *et al.*, *Recommendations for a privacy impact assessment framework for the European Union, PIAF (Privacy Impact Assessment Framework) project*, Grant agreement JUST/2010/FRAC/AG/1137 – 30---CE---0377117/00---70, Deliverable D3, November 2012, pp.26-27, available at http://www.piafproject.eu/Deliverables.html (last accessed on 15 June 2017).

[168] See (including for all quotations in this paragraph) Paul De Hert, Dariusz Kloza, David Wright *et al.*, *Recommendations for a privacy impact assessment framework for the European Union*, *op. cit.*, p.23. In the same sense, see Article 29 Data Protection Working Party, Opinion 04/2013 on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems ('DPIA Template') prepared by Expert Group 2 of the Commission's Smart Grid Task Force (WP 205), adopted on 22 April 2013, p. 13, available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp205_en.pdf (last accessed on 14 June 2017).

4.3 Description of the scope and framework of the study

This step aims at determining all the "*basic parameters within which risks must be managed*"[169].

For that purpose, the following steps must be followed:

4.3.1 Description of the framework of the study

This section includes the study of all the elements that are necessary to the risk management step, namely a description of the frame of the study (which enables to set up the context, to ensure the feasibility of the study, and to orientate works and deliverables based on real objectives), the identification of the assets (which refer to the assets, including immaterial, that need to be protected, and to the supports of these assets - human, hardware, software...), and a preparation of metrics (which are the parameters ans scales which will be used to manage risks).

4.3.1.1 Description of the frame of the study

This description must include the objective of the study, the expected deliberables, and the procedure to be followed.

4.3.1.2 Description of the context of the study

This section must include a description of the external and internal contexts of the study, a definition of the notion of risk in these contexts, and a description of the overall organisation in the area of risk management.

4.3.1.3 Detailed description of the envisionned project or processing operations

The envisionned project and / or the envisionned processing operations must be described in detail, along with their purposes and information flows. The accuracy, completeness and quality of this description are of utmost importance in order to enable an accurate assessment of actual risks.

4.3.1.4 Description of the scope and boundaries of the study

This section must include a description of the scope of the study, a description of the purpose of the study, an identification of the issues of this study/challenges at stake in the general context, a description of the processes involved and an identification of the factors to be eliminated, if any, and a description of the security modes of operation to be chosen.

4.3.1.5 Identification of the parameters to be considered

This action must include an identification of the legal constraints and requirements, and the way the project or the processing operations will meet these requirements. This implies a description of the project in the light of the ECHR and personal data protection requirements (explaining how the project will comply with those sets of requirements), which both imply

[169] This sentence is from the ENISA: ENISA website, Risk Management, Definition of scope and framework, available at http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/rm-process/crm-strategy/scope-framework (home/our activities/risk management/current risk/ rm inventory/rm process/crm strategy/Scope & Framework), last accessed on 15 June 2017.

inter alia an assessment of the necessity and proportionality of the processing operations in relation to the purposes.

During this step must also be identified the internal references on information security, as well as the contraints that are specific to the organism and to the scope of the study. This must lead *inter alia* to identify and analyse the difficulties that the project's features and potentially known end-user expectations may pose in relation to personal data and privacy protection.

4.3.1.6 Identification of the threat sources

This action aims at identifying threat sources, which must be illustrated with concrete examples and which may be associated with additional values such as the frequency of exposure to this threat source, the potential in terms of motivation and capacity for action, its capacity for concealment…. A template that may be used during this step of the assessment is proposed below (with practical examples that need to be adapted). The list of threat sources proposed by the EBIOS base of knowledge[170] should be a source of inspiration.

Example of template that may be used in order to identify threat sources:

Identification of threat sources		
Types of threat sources	**selected or not**	**Example**
Human source, internal, malicious, with low capacities	Yes, some end-user organisations might be exposed to this threat	Maintenance / cleaning staff Analyst (with low level of access authorisation) / Trainee acting playfully or in order to strenghten the combat against organised crime, while breaching data protection rules
Human source, internal, malicious, with significant capacities	Yes, some end-user organisations might be exposed to this threat	Analyst initiative to strenghten the combat against organised crime, while breaching data protection rules Analyst guided by personal reasons (tracking someone in particular; harming the organisation...) Sub-contractor, provider, help-desk agent, who does not respect the contract that imposes no data access and/or storage

Table 1: Example of template that may be used in order to identify threat sources

4.3.2 Identification of the assets

The aim of this step is to identify the assets that are included in the scope of the study. Assets are the goods, resources or values, including immaterial, that need to be protected, and to the elements that support them, which might especially be human, an hardware component or a software.

[170] EBIOS 2010, Expression des Besoins et Identification des Objectifs de Sécurité, ANSSI, 25 October 2011, presentation webpage, available at https://www.ssi.gouv.fr/guide/ebios-2010-expression-des-besoins-et-identification-des-objectifs-de-securite/ (last accessed on 15 June 2017).

4.3.2.1 Primary assets

Primary assets are the non-material resources that need to be protected (for example from unavailability or from a breach of confidentiality). In other words, they consist in non-material resources whose availability, confidentiality and other potential safety criteria (such as integrity) determined in the ad hoc following step (see Section 4.3.3) must be ensured.

In a typical PIA they are firstly the personal data or (depending on the exact nature of the project to be assessed) more largely the data that will be processed by the system or that will result from the system processing's operations.

Ideally, primary asset should also include the legal requirement that must be respected based on the ECHR and the Data Protection Law, at the exception of the requirement of security and confidentiality[171], namely[172]:

- Specific, clear, accessible, stable and foreseeable legal basis.
- Necessity of the project or processing (efficient answer to a pressing social need).
- Proportionality of the answer (strict necessity taking into account the severity of the social need, the proportionnality of the restricted behaviour, the scope of the interference (especially in terms of number of data, of people and places affected, of situations of use of the system/project), and the nature of other answers available).
- Legitimate, specified, explicit, compatible and non-diverted purpose.
- Data quality (fair and lawful processing of accurate, reliable[173] and up-to-date data).
- Minimisation (adequate, relevant and limited to what is necessary[174] to reach the purposes).
- Time limitation (kept for no longer than necessary to reach the purposes), including by the setting-up of time limits *"for erasure or for a periodic review"*[175].
- Data subject consent or other legal ground listed by law.
- Data subject information.
- Data subject rights of access, communication, rectification and erasure.
- Prohibition of decisions based solely on automated processing where they produce legal effects effects concerning the data subject or similarly significantly affect him or her[176].
- DPA notification where required by law.

[171] The legal requirement of security and confidentiality of the processing is not included in the following assets, since security and confidentiality measures aim at ensuring both the efficiency of most of other legal requirements and the security of the system, including the processed data. As a consequence, security and confidentiality measures will be presented in steps 4.3.2.4 and 4.5 of the current methodology.

[172] In relation to the content of these requirements, see Estelle De Marco *et al.*, MANDOLA deliverable D2.2 - *Identification and analysis of the legal and ethical framework*, MANDOLA project (Monitoring ANd Detecting OnLine hAte speech) - GA noJUST/2014/RRAC/AG/HATE/6652, http://mandola-project.eu/, 12 July 2017.

[173] Keepind in mind that the non-reliability of data, which might occur where collecting data on the Internet, must lead to implement appropriate safeguards aiming at protecting individuals' rights.

[174] This formulation is the one of the GDPR. Directive 95/46/EC evokes "non excessive" data, which in essence has the same meaning.

[175] GDPR, recital n°39.

[176] Article 22 of the GDPR.

- Enhanced protection of sensitive data (special catégroie of data listed in the law, in addition to communications, location data and trafic data.
- Adequate level of protection in case of certain data transfer outside the EU, in compliance with law.

These assets might also consist in the fundamental rights that can be impacted by the project and which preservation is not ensured by the legal requirements listed above.

4.3.2.2 Supporting assets

Supporting assets are the components (of a technical nature or not) of the information system, and more widely of information systems involved, which support primary assets. Vulnerabilities of these supporting assets might be exploited or might lead to harm a primary asset. The identification of supporting assets can only be done when primary assets are known, which means that it may be not possible to list them all at the beginning of a project, when they are not already specified. A list of supporting assets, that can be used as a basis of inspiration, is proposed in the "knowledge base" of the EBIOS method[177]. The PIA of the ePOOLICE prototype[178] identified additional ones, namely National, European and International authorities.

4.3.2.3 Links between primary assets and supporting assets

This action aims at determining the links between primary assets and supporting assets, in order to better identify the risks that burden the scope of the study. If practicable taking into account the particular nature of the primary assets, results should be ideally presented in a cross-classification table. A template that may be used during this step of the assessment is proposed below (with practical examples that need to be adapted).

Template that may me used in order to present links between supporting assets and primary assets

Primary assets **Supporting assets**	**(Personal) data / URLs**	**Privacy & DP requirements** (might be divided into 14 columns in order to link each specific requirement to its supporting assets)	**Fundamental rights**
SYS DEP- Computer and telephone systems (dependent from the project authority)	**x**	**x**	
HAR - computers used for visualisation (internal)	x	x	
HAR - Storing server (internal or externally hosted)	x	x	
SOF - ...	x	x	
CTC - ...	x	x	
SYS IND - Computer and information systems, independent from the project authority			**x**

[177] EBIOS 2010, Expression des Besoins et Identification des Objectifs de Sécurité, op. cit. The Knowledge base is specifically accessible at https://www.ssi.gouv.fr/uploads/2011/10/EBIOS-2-BasesDeConnaissances-2010-01-25.pdf.

[178] Estelle De Marco, Nasredine Semmar *et al.*, *Deliverable D3.4 - Final report*, ePOOLICE project (early Pursuit against Organized crime using envirOnmental Scanning, the Law and IntelligenCE systems), projet n° FP7-SEC-2012-312651, version 1.4 of 28 December 2015 (Doc. ID EPO-1512-WP03-004-V1.4-DV-RE), Section 4 (PIA of the ePOOLICE prototype), available at https://www.epoolice.eu/ (last accessed on 15 June 2017).

...SOF - Social network analysed by the project's features			x
ORG - organisation	**x**	**x**	
PER - Analyst/staff members authorised to access the system	x	x	
PER - Providers authorised to access the system	x	x	
PAP - ...	x	x	
CHA - ...		x	
PRE - End-user organisation premises	**x**	**x**	
OPE IND - Organisations and persons, independent from the project authority		**x**	**x**
PAR - Parliament		x	
JUD - Judiciary		x	
IND - Independent authorities		x	
ADM - Administrative authorities		x	
PER - Fundamental rights holders	x		x

Table 2: Example of template that may be used in order to determine links between supporting assets and primary assets

4.3.2.4 Existing security and compliance measures

This action consists in identifying all the security measures that are already implemented on supporting assets. These measures include, within the framework of the PIA of a system that may impact privacy and personal data:

- All the measures that are or must be implemented (by design and by default where feasible[179]) to ensure compliance with legal requirements and to ensure the preservation of the rights and freedoms of individuals, including the risk of discrimination. These measures are supposed to be detailed in the step of the PIA that is relating to the parameters to be considered.
- The list of the security measures already implemented at the organisation level and which will be applicable to the system to be implemented. A list of generic security measures, that can be used as a basis of inspiration, is proposed in the "knowledge base" of the EBIOS method[180].
- Ideally, since this will become mandatory once the new EU GDPR and Directive on personal data protection for the police and criminal justice sector will be applicable, the list of mechanisms designed to demonstrate compliance with the Regulation or the Directive, depending on the applicable instrument.

4.3.3 Preparation of metrics

This step aims at determining the parameters and scales that will be used to manage risks.

[179] Keeping in mind that privacy by design and by default will be mandatory once the new GDPR will be applicable.

[180] EBIOS 2010, Expression des Besoins et Identification des Objectifs de Sécurité, *op. cit*.

4.3.3.1 Definition of the safety criteria and of the scale of needs

Safety criteria are at least the availability of primary assets, their integrity, and their confidentiality. Other safety criteria may be determined.

Consequently, the scale of need must specify the needs in term of (at least) availability, integrity, and confidentiality, for each primary asset. This analysis must be done at the same time as the identification of the primary assets (see previously), since the determination of the safety criteria and of the scale of needs are closely tied to the nature of these assets, in general and in particular in a project such as the MANDOLA one. Templates that may be used during this step of the assessment are proposed below (with practical examples that need to be adapted).

Template that may be used in order to determine safety criteria

Safety criteria	Definition
Availability	Availability of primary assets at the desired time for authorised personnel
Integrity	Accuracy and completeness of primary assets
Confidentiality	Accessibility of primary assets to authorised persons only

Table 3: Example of template that may be used in order to determine safety criteria

Template that may be used in order to express safety needs in terms of availability

Levels of the scale	Description of the scale
6. 0 h	The primary asset must not be unavailable
5. Less than 4 h	The primary asset must be available within 4 hours
4. Less than 24 h	The primary asset must be available within 24 hours
3. Less than 72h	The primary asset must be available within 72 hours
2. Less than 2 weeks	The primary asset can be unavailable more than 72 hours but must be recovered within a reasonable time (maximum of 2 weeks).
1. More than 2 weeks	The primary asset can be unavailable more than 2 weeks.

Table 4: Example of template that may be used in order to express safety needs in terms of availability

Template that may be used in order to express safety needs in terms of integrity

Levels of the scale	Description of the scale
3.Integrity	The primary asset must have a rigorous integrity
2.Controlled	The primary asset may have an integrity issue if it is discovered and if the integrity is recovered
1.Detectable	The primary asset may have an integrity issue if it is discovered

Table 5: Example of template that may be used in order to express safety needs in terms of integrity

Template that may be used in order to express safety needs in terms of confidentiality

Levels of the scale	Description of the scale
7.Highly confidential	The primary asset must only be accessible to one or a thin number of entitled persons in restricted situations (ex. persons authorised to search for information

	related to a particular name, in order to enable the exercise of a data subject's right of access)
6.Confidential	The primary asset must only be accessible to authorised persons on a need-to-know basis in specific situations (ex. persons authorised to access the originating URLs stored in the database)
5.Private	The primary asset must only be accessible to authorised persons on a need-to-know basis (ex. persons authorised to access data stored in the database, which can be of a personal nature)
4.Restricted level 2	The primary asset must only be accessible to authorised persons (ex. persons authorised to see full results of one given visualisation tool)
3.Restricted	The primary asset must only be accessible to involved personnel (ex. persons authorised to use a visualisation tool)
2.Limited	The primary asset must only be accessible to the staff and authorised partners or providers (ex.: maintenance personnel)
1.Public	The primary asset is public

Table 6: Example of template that may be used in order to express safety needs in terms of confidentiality

4.3.3.2 Determination of the severity scale

The aim of this sub-step is to determine the level of severity that will be associated with feared events and risks. In other words, the aim is to determine all the possible levels of severity that impacts may have on the rights and freedoms of individuals. The severity of these impacts may be determined, where relevant and following previous recommendations of the French Data protection Authority[181], according to the identifying capacity of a personal data, and according to the harmful nature of the impact for individuals. A template that may be used during this step of the assessment is proposed below (with practical examples that need to be adapted).

Template that may be used in order to determine the scale of the severity of feared events and risks

Levels of the scale	Impact aspects	Description of the scale
4.Critical	Harmful nature	Concerned persons might suffer significant inconvenience, even irreparable, which they might not be able to overcome (financial peril such as important debts or inability to work; long-lasting illness, death...).
	Identifying capacity	It seems extremely easy to identify someone with the concerned data (ex. first name, surname, date of birth and postal address at one given

[181] Before the publication of its current PIA manual, the CNIL had published in 2012 a guide aiming at managing risks on privacy, also based on the EBIOS method (CNIL, *Gérer les risques sur les libertés et la vie privée, the method*, June 2012, https://www.cnil.fr/sites/default/files/typo/document/CNIL-Guide_Securite_avance_Methode.pdf). This guide of 2012 was advising to determine the severity of impacts according to the identifying capacity of a personal data, and according to the harmful nature of the impact for individuals. In its new PIA manual, the CNIl advises only to take into account "*primarily estimated in terms of the extent of potential impacts on data subjects*", and to raise or lewer the severity level "*by including additional factors*" such as "*level of identification of personal data*", "*nature of risk sources*", "*number of interconnections (especially with foreign sites)*", "*number of recipients (which facilitates the correlation between originally separated personal data)*": see the CNIL PIA manual 2 - Tools, respectively pp. 13 and 15, https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-2-Tools.pdf. However, we think that assessing the severity of impacts according both to the identifying capacity of a personal data and according to the harmful nature of the impact for individuals is still relevant, the other new parameters retained by the CNIL appearing to be more difficult to assess (since they mostly relate to the potential number of recipients and/or of uses following a breach to confidentiality, which might be very difficult to figure out). URLs last accessed on 15 June 2017.

		country's population-wide).
3.Important	Harmful nature	Concerned persons might suffer significant inconvenience, which they will be able to overcome, but with serious difficulties (misappropriation if funds, banking ban, damage to property, job loss, law suit, worthening state of health...).
	Identifying capacity	It seems relatively easy to identify someone with the concerned data (ex. first name, surname and date of birth at one given country's population-wide).
2.Limited	Harmful nature	Concerned persons might suffer significant inconvenience, which they will be able to overcome despite some difficulties (additional costs, refusal of access to commercial services, fear, misunderstanding, stress, minor ailment…).
	Identifying capacity	It seems difficult to identify someone with the concerned data but it might happen (ex. first name and surname at one given country's population-wide).
1.Negligible	Harmful nature	The impact on individuals will be weak; inconveniences will be overcome without difficulty (ex.: waste of time in order to perform a given action, irritation...).
	Identifying capacity	It seems nearly impossible to identify someone with the concerned data (ex. first name only at one given country's population-wide).

Table 7: Example of template that may be used in order to determine the severity scale

4.3.3.3 Determination of the likelihood scale

The aim of this step is to create a scale of levels of likelihood, to be associated with threat scenarios. This scale should ideally take into acount both the ability of the source to act and the vulnerability of the supporting asset. A template that may be used during this step of the assessment is proposed below (with practical examples that might need to be adapted).

Template that may be used in order to determine the scale of likelihood of threat scenarios

Levels of the scale	Description of the scale
4.Maximal	That certainly will occur / The supporting asset is very vulnerable
3.High	That should occur / The supporting asset is vulnerable
2.Significant	That may occur / The supporting asset might be vulnerable
1.Minimal	That should not occur / There is a very low vulnerability of the supporting asset

Table 8: Example of template that may be used in order to determine the likelihood scale

4.3.3.4 Determination of the risk management criteria

This action aims to determine the rules that will be used to make decisions during the course of the assessment, regarding the evaluation and the treatment of risks. Since these rules reflect *inter alia* the caracteristics of the organisation in charge of the processing (constraints objectives, values…), the particular nature of the data that are processed, and the particular nature of the impacts to be avoided, these criteria should be determined as the assessment progresses. A template that may be used during this step of the assessment is proposed below (with practical examples that might need to be adapted).

Template that may be used in order to determine the risk management criteria

Action	**Risk management criteria (rule chosen to carry out the action))**
Estimation of feared event	The severity of feared events is estimated by using the scale provided for to that effect. In addition, where security measures or measures aiming to ensure compliance with law are already implemented: ▪ with the highly probable effect of limiting the severity of the feared event, the severity will be estimated a level lower. ▪ with the highly probable effect of eliminating the severity of the feared event, the severity will be estimated at the lowest level.
Evaluation of feared event	The likelihood is estimated taking into account both the ability of the source to act and the vulnerability of the supporting asset, using the scale provided for to that effect. Where several levels of likelihood are identified depending on the threat's source, the maximum value is retained. In addition, where security measures or measures aiming to ensure compliance with law are already implemented: ▪ with the highly probable effect of limiting the likelihood of the feared event, the likelihood will be estimated a level lower. ▪ with the highly probable effect of preventing the feared event to occur, the likelihood will be estimated at the lowest level.
Estimation of risks	The severity of a risk is equal to the severity of the considered feared event. The likelihood of a risk is equal to the maximal likelihood of all threat scenarios that are linked to the considered feared event.
Evaluation of risks	Risks which severity is critical, and risks which severity is important and likelihood high or maximal, are considered as being intolerable. Risks which severity is important and which likelihood is significant, and risks which severity is limited and which likelihood is high or maximal, are considered as being significant. Other risks are considered as being negligeable.

Table 9: Example of template that may be used in order to determine risk management criteria

4.4 Assessment of the risks to fundamental rights and freedoms

The assessment of the risks to fundamental rights and freedoms implies to study both feared events and threat scenarios before performing a risk analysis.

4.4.1 Study of feared events

This sub-step aims to identify the events that are to be prevented, in relation with the preservation of primary assets.

Feared events are events that threaten security needs (i.e., for example, the need for a high or moderate confidentiality or integrity of a given primary asset, such as certain categories of processed data). The identification of feared event must take into account, *inter alia*, potential end-users expectations and stakeholders opinions collected during step 4.6 of the current method.

As a first step, security needs must be identified for each safety criteria of each primary asset, by chosing the lowest value that is still acceptable. For example, a specific primary asset may suffer from a lack of integrity for a short period of time if the integrity is afterward recovered, while a confidentiality issue cannot be tolerated. In this case, according to metrics prepared in Section 4.3.3.1 of the current method, the safety needs in terms of integrity will be “controlled” whereas the safety needs in terms of confidentiality will be “highly confidential”.

A second step must be the identification of the impacts that would occur in case the security needs are not respected. Examples of these impacts must be given, and the severity of these impacts must be estimated, using the scale and risk management criteria prepared on this purpose. As already explained, this severity may be estimated taking into account the value of the targeted primary asset or the identifying capacity of this primary asset and the severity of the impact itself for individuals[182] (because the impact is high or because it can occur several times). A list of types of impacts, which may be used as a basis of inspiration, is proposed in the "knowledge base" of the EBIOS method[183].

This assessment will be performed both without consideration of and taking into account existing measures that aim to control the feared events and to ensure compliance with legal requirements (the latter forming part of primary assets in the current method). Indeed, both these measures might already be appropriate to lower the likelihood or the severity of the feared event, since they may have the effect, as indicated in the EBIOS method[184] in relation with existing security measures, of protecting the security needs of primary assets (these measures are mainly prevention and recovery measures), of reducing identified impacts (prediction and preparation, prevention, containment, fight, recovery, restoration, compensation…), of counteracting each identified threat source (prediction and preparation, deterrence, detection, containment…), of ensuring protection against threats (these measures are mainly detection and protection measures), and of reducing supporting assets' vulnerabilities (these measures are mainly prevention and protection measures).

In that case, as already determined in the subsection dedicated to risk management criteria, where security measures or safeguards are already implemented with the effect of limiting or even eliminating the likelihood or the severity of a feared event, this likelihood or severity will be estimated, respectively, a level lower or at the lowest level.

A template that may be used during this step of the assessment is proposed below (with practical examples that might need to be adapted).

Finally, each feared event may be evaluated, to classify all the feared events according to their importance. This step is optional since it could be not appropriate for all kind of primary assets (for instance, compliance with law is always important and the different legal requirements may not be classifed according to their importance).

[182] See Section 4.3.3.2. and the previous footnote.

[183] EBIOS 2010, *Expression des Besoins et Identification des Objectifs de Sécurité*, Base de connaissance (knowledge base), https://www.ssi.gouv.fr/uploads/2011/10/EBIOS-2-BasesDeConnaissances-2010-01-25.pdf (last accessed on 15 June 2017).

[184] EBIOS 2010, *Expression des Besoins et Identification des Objectifs de Sécurité*, Guide méthodologique (methodological guide), p. 62, https://www.ssi.gouv.fr/uploads/2011/10/EBIOS-1-GuideMethodologique-2010-01-25.pdf (last accessed on 15 June 2017).

Template that may be used in order to study feared events

Feared event	Security need (value)	Impact (examples)	Severity of the impact on individuals	Existing measures that could reduce the severity	Severity final assessment
Originating URLs (identifying capacity: potentially critical)					
Unavailability	3 (less than 72)	Right of access might be impossible to exercise; Impossibility for end-users to verify the reliability of a pers. data linked to this URL (may drive to bad strategic decisions in case the system has such aim).	1 (negligible)	Safeguard n°x may prevent any harm caused by the impossibility to verify a source's reliability. Safeguard n°y may prevent misuses.	1 (negligible)
Integrity compromission	1 (detectable)	Right of access impossible to exercise ; Impossibility for end-users to verify the reliability of a pers. data linked to this URL.	1 (negligible)	No measure particularly planned. Safeguard n°x may prevent any harm caused by the impossibility to verify a source's reliability.	1 (negligible)
Confidentiality breach	6 (confidential)	Data misuse (individual's identification).	3 (important)	Safeguard n°z.	2 (limited) - impacts might be important but cases should be limited.
Data relating to Internet users (identifying capacity: unknown)					
Unavailability					
Integrity compromission					
Confidentiality breach					
...					
Unavailability					
Integrity compromission					
Confidentiality breach					

Table 10: Example of template that may be used in order to study feared events

4.4.2 Study of threat scenarios

This analysis and the previous one may take place on a sequential manner but may also take place at the same time and with the help of the same template, since the analysis of feared events and the analysis of threat scenarios are closely linked.

This action aims at identifying threat scenarios that can burden a supporting asset and be at the origin of a feared event (feared event that may lead, as seen previously, to prejudice the security need of a primary asset).

It is necessary in this step to identify the threat sources (in other words the agents that may threaten supporting assets), the threats that could occur (in other words the possible actions of these sources on supporting assets), and the vulnerabilities of supporting assets that may allow these threats to occur. These three elements form together a threat scenario.

A list of types of threat sources and a list of generic threats and vulnerabilities, which may be used as a basis of inspiration, are proposed in the "knowledge base" of the EBIOS method[185] and in the CNIL's security guide[186].

As already said in the previous subsection, this assessment will be performed both without consideration of and taking into account existing measures that aim to control the feared events and to ensure compliance with legal requirements (the latter forming part of primary assets in the current method). Indeed, both these measures might already be appropriate to lower the likelihood or the severity of the feared event, since they may have the effect, as indicated in the EBIOS method[187] in relation with existing security measures, of protecting the security needs of primary assets (these measures are mainly prevention and recovery measures), of reducing identified impacts (prediction and preparation, prevention, containment, fight, recovery, restoration, compensation…), of counteracting each identified threat source (prediction and preparation, deterrence, detection, containment…), of ensuring protection against threats (these measures are mainly detection and protection measures), and of reducing supporting assets' vulnerabilities (these measures are mainly prevention and protection measures).

A template that may be used during this step of the assessment is proposed below (with practical examples that might need to be adapted).

Finally, each threat scenario may be evaluated, to classify all the scenarios according to their likelihood. This step is optional since it could not be appropriate for all kind of primary assets (for example, depending on the nature of the data that are processed, the risk assessment may or may not conclude that some risks, even if they have a low level of probability, must not be taken into account).

[185] EBIOS 2010, Expression des Besoins et Identification des Objectifs de Sécurité, ANSSI, 25 October 2011, available at https://www.ssi.gouv.fr/guide/ebios-2010-expression-des-besoins-et-identification-des-objectifs-de-securite/ (last accessed on 15 June 2017).

[186] Cnil, *Privacy Impact Assessments: the CNIL publishes its PIA manual*, 10 July 2015, PIA Manual 1 - Methodology, p. 16, https://www.cnil.fr/fr/node/15798.

[187] EBIOS 2010, *Expression des Besoins et Identification des Objectifs de Sécurité*, Guide méthodologique (methodological guide), *op. cit.* p. 62.

Template that may be used to study threat scenarios

Feared event	Threat source	Probable threats (action)	Likelihood			Existing measures that could reduce the likelihood	Likelihood final assessment
			Source's ability to act	Supporting asset vulnerability	Total		
Originating URLs							
Unavailability	-Internal human error (analyst, computer scientist, provider) -External malicious human source (hacker, activist...) -Malicious code of unknown origin -Internal event (computer failure, maintenance error...) - may be or not due to a natural event	-Hardware deterioration or modification -Deletion of part or all of a software or of data -Software or data modification	2 (significant)	2 (significant)	2	No measure	2
Integrity compromission	-Internal human error (analyst, computer scientist, provider) - ...	-Hardware deterioration or modification -Deletion of part or all of a software or of data - ...	2 (significant)	2 (significant)	2	No measure	2
Confidentiality breach	-Internal human error (analyst, computer scientist, provider) - ...	-Hardware deterioration or modification -Deletion of part or all of a software or of data -Software or data modification - non-observance of security levels - ...	3 (High)	3 (High - ORG) to 2 (significant - SYS DEP, PRE)	3	No measure	3
Personal data relating to Internet users							
Unavailability							
Integrity compromission							
Confidentiality							

breach							
…							
Unavailability							

Table 11: Example of template that may be used in order to study threat scenarios

4.4.3 Risk analysis

This step aims primarily at analysing risks. A risk is the combination of a feared event with a threat scenario. Therefore, if not decided otherwise in the risk management criteria, the severity of a risk corresponds to the severity of the feared event, and the likelihood of this risk corresponds to the likelihood of the relating threat scenario.

A template that may be used during this step of the assessment is proposed below and (with practical examples that need to be adapted). This template may be merged with the templates proposed within the framework of the two previous steps.

In addition,each risk may be evaluated, in order to classify all the risks according to their importance (a template that may be used for this purpose is proposed below (with practical examples that need to be adapted). This step is optional, for the reasons explained in the two previous steps. Risks may also be represented graphically (likelihood in x axis and severity in y axis).

In this risk analysis step, it is also usually recommended, in traditional risk assessment methods, to chose the risk treatment options between risk avoidance (which means modifying the context to eliminate the risk), risk reduction (which means reducing the impacts or the likelihood), risk maintenance (which means accepting the consequences of risks and not taking treatment measures) and risk transfer (which means *inter alia* transfering the responsibility of mitigating the risk to a third party). However, regarding privacy and personal protection issues, such a choice may be not relevant in situations where avoidance corresponds to a legal requirement. Therefore, this sub-step may be performed or not, depending on its overall relevance.

Finally, it is usually recommended, in traditional risk assessment methods, to identify and estimate (in terms of severity and likelihood) the risks that remain once each security aim is reached, and to verify that these risks are accepted with full background knowledge. These risks may be reduced later, once the other risks are treated. For the same reason as the one explained in the previous paragraph, the performance of this sub-step may be relevant or not, depending on the nature of the risks that have been identified.

Template that may be used in order to assess risks

Feared event	Threat source	Threat (action)	Severity of the impact	Likelihood of the threat scenario	Risk assessment
Originating URLs					
Unavailability (risk D1a)	-Internal human error (analyst, computer scientist, provider) -External malicious human source (hacker, activist...) -Malicious code of unknown origin -Internal event (computer failure, maintenance error...) due or not to a natural event	-Hardware deterioration or modification -Deletion of part or all of a software or of data -Software or data modification	1	2	1 (N)
Integrity compromission (risk D1b)	-Internal human error (analyst, computer scientist, provider) -External malicious human source (hacker, activist...) -Malicious code of unknown origin - **...**	-Hardware deterioration or modification -Deletion of part or all of a software or of data -Software or data modification	1	2	1 (N)
Confidentiality breach (risk D1c)	Internal human error (analyst, computer scientist, provider) -Internal malicious human source (analyst, computer scientist, provider) -External malicious human source (hacker, activist...) - **...**	-Hardware deterioration or modification -Deletion of part or all of a software or of data -Software or data modification - non-observance of security levels - Sotware function creep - Lack of awareness/training of analyst and/or their hierarchy	2	3	2 (S)
Personal data relating to Internet users					
Unavailability (risk D2a)					
Integrity compromission (risk D2b)					
Confidentiality breach (risk D2c)					
...					
Unavailability (risk D3a)					

Legend - (reminder of risk management criteria):

(1) Negligible

(2) Significant

(3) Intolerable

Table 12: Example of template that may be used in order to assess risks

Template that may be used in order to evaluate risks

1 (N) Negligible risks	2 (S) Significant risks	3 (I) Intolerable risks

4 Critical	Risk linked to the unavailability and integrity compromission of the data minimisation requirement **(risks n°5, 7)**	Risk linked to the unavailability and integrity compromission of the explicit, specified and legitimate purposes requirement **(risks n° 2, 6)** **... (risks n° ...)** **... (risk n°...)**	Risk linked to the confidentiality breach and integrity compromission of personal data rel. to end-users **(risks n° 8, 9)** **... (risks n° ...)**	**... (risks n° ...)**
3 Important	**... (risk n° ...)**	Risk linked to the unavailability and integrity compromission of the prohibition of decisions based solely on automated processing **(risks n°1, 12)** **... (risks n°...)**	Risk linked to the unavailability of personal data rel. to end-users **(risk n°9)** **... (risk n° ...)**	**... (risk n° ...)**
2 Limited	**... (risks n° ...)**	Risk linked to the integrity compromission of personal data rel. to Internet users **(risk 16)** Risk linked to the unavailability and integrity compromission of the time limitation requirement **(risks n°18, 20)** **... (risk n° ...)**	Risks linked to the confidentiality breach of originating URLs **(risk n°17)** Risk linked to the confidentiality breach of personal data rel. to Internet users **(risk n°19)** **... (risk n° ...)**	**... (risk n° ...)**
1 Negligeable	**... (risk n° ...)**	**... (risk n° ...)**	**... (risk n° ...)**	**... (risk n° ...)**
Severity **Like lihood**	**1 Minimal**	**2 Significant**	**3 High**	**4 Maximal**

Table 13: Example of template that may be used in order to evaluate risks

4.5 Risk treatment

This step aims at determining the means to treat identified risks, taking into account the constraints that are specific to the project, notably of a technical nature.

These measures can be determined using the base of knowledge proposed in the EBIOS method[188] and some examples proposed in the CNIL's PIA method[189]. However, these measures must primarily be determined by analysing results of the three previous steps (study of feared events, study of threat scenarions, and risk analysis). Ideally, these three steps and the current one should be performed at the same time.

For each identifed measure, it may be useful to determine the line of defense to which it belongs (prevention, protection or recovery). For each line of defense, for a better clarity of the presentation of risk assessment results, it might be interesting (depending on these latter results) to identify the category of assets on which the defense applies (for example personal data, legal requirements and other fundamental rights). Bracketed notes

[188] EBIOS 2010, Expression des Besoins et Identification des Objectifs de Sécurité, ANSSI, 25 October 2011, op. cit.

[189] CNIL, *Privacy Impact Assessments: the CNIL publishes its PIA manual*, 10 July 2015, https://www.cnil.fr/fr/node/15798 (last accessed on 15 June 2017).

accompanied with a legend may enable to be even more specific for a better understanding of results.

Ideally, in order to follow risk assessment methods, identified risks should be counteracted by risk treatment measures that belong to at least these three lines of defense[190].

In addition to the determination of risk treatment measures, this step might be the occasion - if this is likely to provide a better clarity of retained measures as a whole - to summarise the measures determined in step 4.3.2.4, which are designed to ensure the protection of personal data and to demonstrate compliance with law, knowing that results of the risk treatment step may lead to reconsider existing or already planned measures, to replace them by more appropriate ones.

A template that may be used during this step of the assessment is proposed below (with examples that need to be adapted).

Moreover, it is adviced to identify and estimate (in terms of severity and likelihood), where relevant, the risks that will remain once each security measures will be implemented, and to verify that these risks are accepted with full background knowledge. Acceptation must be duly justified.

Finally, a plan of action must be drawn up. It must *inter alia* include a description of the way data protection by design and default practices will be implemented.

Template that may be used to formalise chosen risk treatment measures

Description of the measure	Measure's function									Related risks	Mesure's nature		
	Prevention (pers. data -PD)	Prevention (legal requirements - LR)	Prevention (fund. rights - FR)	Protection (PD)	Protection (LR)	Protection (FR)	Recovery (PD)	Recovery (LR)	Recovery (FR)		Technical	Organisational	Legal
Proposed risk treatment measure n°1	x	x								R1, R4, R5		x	
Proposed risk treatment measure n°2													
Proposed risk treatment measure n°3													

Table 14: Example of template that may be used in order to formalise chosen risk treatment measures

4.6 Stakeholders consultation

This step consists in the consultation of relevant stakeholders who might be impacted by the project or who might bring their expertise to the identification of the risks presented by the project, in order to gather their views. According to the research consortium of the PIAF EU

[190] See for example EBIOS 2010, Expression des Besoins et Identification des Objectifs de Sécurité, *op. cit*.

project, the objective is to achieve a "'*win-win' result so that everyone benefit*"[191], which is one of the principles of the privacy by design approach.

Ideally, these stakeholders must be interviewed on the used method and on the intermediate resuls of the PIA, including identifed risks (of which they might in particular extend the list) and proposed mitigations measures.

These views must be taken in consideration, which might lead to modify the conclusions of certain steps of the PIA already performed. In case the PIA results include recommendations (especially of use, of implementation or of new developments), which might for example occur where the project's outcomes are intended to be used by organisations that are different from the project development organisation, these recommendations might be refined, modified or extended based on the results of this stakeholders consultation.

The MANDOLA consortium plans to consult the members of the Advisory board, who belong to several areas of activity (law enforcement, education, industry, civil society combatting illegal online content) and have different but complementary competencies (including technical, legal and ethical).

4.7 Monitoring and review

The findings of the study must be subjected to internal validation, and to an external audit or review. Ideally, the PIA and its results should be published, primarily in order to enhance trust in the project's results, transparency and accountability of data controllers. In case the PIA highlights that the project "*reveals high residual risks*"[192], the relevant data protection authority must be consulted prior any personal data processing, according to the GDPR and the Directive on personal data protection for the police and criminal justice sector[193], and ideally prior any implementation or use of the project's outcomes.

In addition, the implementation of the measures must be monitored, and mechanisms must ensure that the PIA remains relevant and updated. Especially, the PIA should be revisited each time a modification is brought to the project or processing that has been assessed, the Article 29 data protection working party providing examples of situations which require a new PIA[194]. In addition, a compliance review must be conducted regularly, at the latest three years after the carrying out of the PIA, as adviced by the Article 29 data protection working

[191] Paul De Hert, Dariusz Kloza, David Wright *et al.*, *Recommendations for a privacy impact assessment framework for the European Union, PIAF (Privacy Impact Assessment Framework) project*, Grant agreement JUST/2010/FRAC/AG/1137 – 30---CE---0377117/00---70, Deliverable D3, November 2012, p. 29, available at http://www.piafproject.eu/Deliverables.html (last accessed on 15 June 2017).

[192] Article 29 Data Protection Working Party, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679* (WP248), 4 April 2017, p. 17, http://ec.europa.eu/newsroom/document.cfm?doc_id=44137 (last accessed on 15 June 2017).

[193] Art. 36, 1 of the GDPR ; article 26, 1, a of the Directive on personal data protection for the police and criminal justice sector.

[194] Article 29 Data Protection Working Party, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679* (WP248), *op. cit.* p. 12. These situations are especially those where there is a "*change to one of the components of the processing operation (data, supporting assets, risk sources, potential impacts, threats, etc.) or (...) (where) the context of the processing evolves (purpose, functionalities, etc.)*". A new PIA is also required, for example, where "*the organisational or societal context for the processing activity has changed, for example because the effects of certain automated decisions have become more significant, new categories of natural persons become vulnerable to discrimination or the data is intended to be transferred to data recipients located in a country which has left the EU*".

party[195]. A new PIA will be needed, in any case, at the time the future EU data protection legal framework will be applicable, in order to ensure compliance with the provisions of this new EU legal framework as well as with applicable domestic laws that will be adopted in order to ease and complement the implementation of the General Data Protection Regulation and to transpose the Police Directive (where applicable to the assessed project or a part of it).

During the MANDOLA project, the monitoring and review task - whose ideal content has been described above, cannot be performed comprehensively given the particularities of this project.

The PIA internal validation will be done by all the MANDOLA partners, before being submitted to an ethical and quality review, as other MANDOLA deliverables. The deliverable including the PIA of the MANDOLA outomes will be published and submitted to the European Commission, but the context and framework of the MANDOLA project do not lend themselves well to an additional external audit.

The PIA of the MANDOLA outcomes will be used in order to implement privacy by design measures to the utmost possible extent, as well as to issue recommendations of use that will target all discovered weaknesses in terms of impact on fundamental rights. However, most of the MANDOLA outcomes are intended to be used by other entities and organisations. As a result, at the end of the MANDOLA project, new PIAs will have to be carried out by these entities and organisations, in order to take into account the new contexts of use of these outcomes (which are unknown to the MANDOLA research consortium). Monitoring measures and mechanisms designed to ensure that the PIA remains relevant and updated will also have to be designed and implemented by these latter entities and organisations.

[195] Article 29 Data Protection Working Party, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679* (WP248), *op. cit.* p. 12.

5 Conclusions

The proposed PIA method concentrates points of agreement between most of existing PIA and DPIA methods and guidelines, and is supplemented with best practices and with requirements that appear appropriate within the framework of an ethical approach, in order to ensure that the results of the PIA of the MANDOLA outcomes will take account of potential risks for rights and freedoms to the utmost possible extent. Results of the application of this method to the MANDOLA outcomes will be presented in the MANDOLA deliverable D2.4b - Final.

6 List of main acronyms and abbreviations

DPIA: Data protection impact assessment.

GPDR or "General Data Protection Regulation": refers to Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC[196].

PIA: Privacy impact assessment.

Police Directive or "Directive on personal data protection for the police and criminal justice sector": refers to the Directive (EU) 2016/680 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA[197].

[196] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:FULL (last accessed on 12 May 2017).

[197] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0089.01.ENG&toc=OJ:L:2016:119:FULL (last accessed on 12 May 2017).