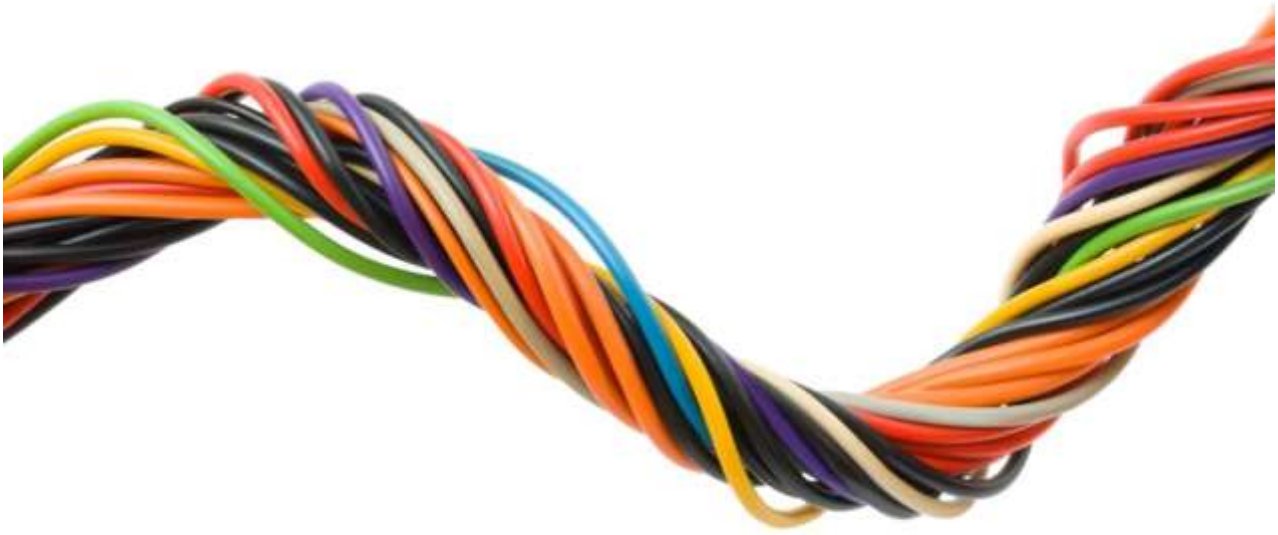
Intended for
ENISA

Document type
Case Study Report

Date
May 2016

EVALUATION OF ENISA'S ACTIVITIES

CASE STUDY REPORT – WORK PACKAGE 3.3 2015



RAMBØLL

EVALUATION OF ENISA'S ACTIVITIES
CASE STUDY REPORT – WORK PACKAGE 3.3 2015

Revision	**1**
Date	**27/05/2016**
Made by	**Ida Maegaard Nielsen**
Checked by	**Karin Attström**
Approved by	**Helene Urth**
Description	**Case study Report – Work Package 3.3 2015**

Ramboll
Square de Meeûs 35,
1000 Brussels
Belgium
T +32 (0)2 737 96 80
F +32 (0)2 737 96 99
www.ramboll.com

CONTENTS

TABLE OF FIGURES AND TABLES

APPENDICES

1. INTRODUCTION

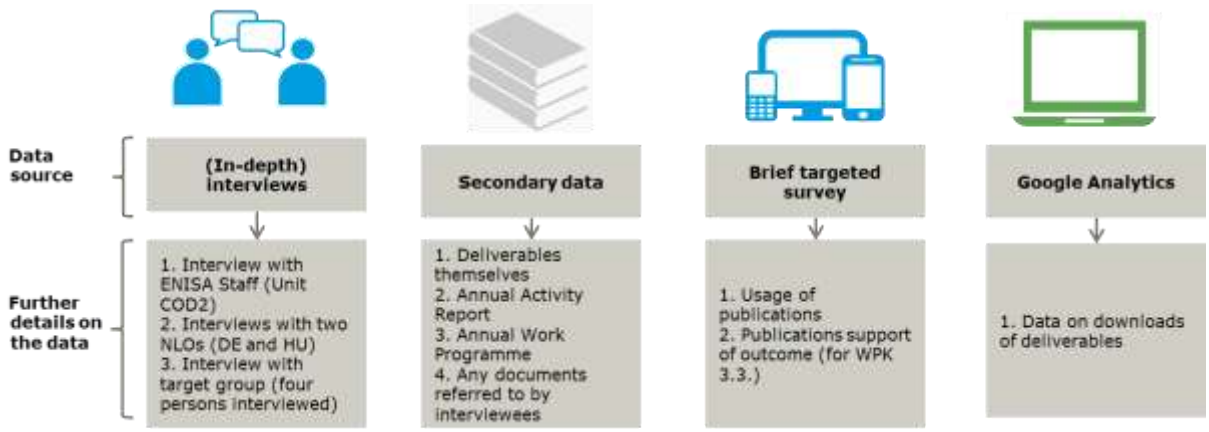
The present report is part of the external evaluation of ENISA's activities in 2015. It takes an in-depth look at one of ENISA's work packages (WPK), namely WPK 3.3: *Assist EU Member States and the Commission in the implementation of NIS measures of EU data protection regulation*. It is one of four WPKs which were intended to contribute to ENISA´s 2015 work programme´s assistance of the Member States and the Commission in developing and implementing the policies necessary to meet the legal and regulatory requirements of Network and Information Security (Strategic Objective 3 (SO)). This case study report presents a detailed analysis of the extent to which WPK 3.3 has done so. In addition, the findings of this report feed into the answering the evaluation questions as summarised in the evaluation matrix.

In total, three case studies were conducted to evaluate ENISA's 2015 activities. They each focus on one of the work packages under Strategic Objectives 1 to 3 (SOs). In our selection of work packages (WPK) we have prioritised those with the highest allocation of funds for SO1 and SO2, and for SO3 we have selected the WPK with the second-highest allocation of funds, but which covers other types of tasks which the Agency undertakes. Thereby, we ensure a diverse coverage of ENISA´s tasks as set out in the basic Regulation, Article 3. Within the three selected WPKs, we include all deliverables above €30,000 (in accordance with the framework for the evaluation).

The case study on WPK 3.3 covers the following two deliverables (with a budget above €30,000):
- D1 - Readiness analysis for the adoption and evolution of privacy enhancing technologies
- D4 - State-of-the-art analysis of data protection in big data architectures

The case study report is based on four sources of data in order to ensure as detailed an examination as possible. The figure below provides an overview of these four sources.

Figure 1: Overview of data sources



With regard to the **in-depth interviews,** a total of 9 persons were interviewed including ENISA staff (COD2), two NLOs, and persons from the target group (Data Protection Authority (DPAs), Academia, a PSG member and a member of staff from FRA).

The **brief targeted survey** was annexed to the general survey on ENISA's 2015 activities. In total, 84 responses were collected and used in the analysis of WPK 3.3. A full overview of the responses to the survey (including the brief targeted survey) can be found in annex 11 to the evaluation report. The interview guide for the case study is presented in annex 10. The **secondary data** (including publications from ENISA) and the **Google Analytics** have been provided to the evaluator by ENISA.

This case study report is organised as follows:
- Section 2 presents the work package and its deliverables, linking them to the outputs, outcomes and results identified in the intervention logic.

- Section 3 presents the findings for the two deliverables with regards to the intended outputs and outcomes based on interviews, survey and the Google Analytics. Based on these findings, an assessment of results is made.
- Section 4 provides conclusions on output, outcome and result level.

2. BACKGROUND

This chapter presents the overall aim of WPK 3.3 and its specific deliverables, their intended outputs, outcomes and results as identified in the intervention logic.

By implementing the activities under SO3, ENISA aims to assist the Member States and the Commission in developing and implementing the policies necessary to meet the legal and regulatory requirements of Network and Information Security. In its work programme, ENISA commits to helping Member States and the Commission with implementing privacy and data protection measures through privacy strategies and new business models. In doing so a two-fold approach is applied, namely 1) providing feedback from an operational perspective to those working on developing the legislative framework and 2) identifying the most cost-effective methods and tools which can support implementation of regulation, including by identifying gaps between these tools and the legislative proposals.

In this context, WPK 3.3 aims to strengthen the Agency´s efforts in the field of privacy and trust by providing analysis of the readiness of the industry, public and private sectors for the adoption and evolution of privacy technologies, which feeds directly into the fourth overall goal of SO3, namely analysing the use of privacy enhancing technologies (PETs). In addition, the WPK also supports ENISA´s objective to provide a state-of-the art analysis of the data protection threats, risks and protection measures in the emerging big and open data landscape. In its approach, ENISA uses the WPK 3.3 activities to build a bridge between data protection legislation and the actual protection mechanisms. This is exemplified by the third annual privacy forum (an activity under this work package) which intended to support policy makers in understanding the technological advances and the research community and industry´s understanding of legislative requirements to technology.

2.1 Deliverables of the work package

2.1.1 Deliverable 1: Readiness analysis for the adoption and evaluation of privacy enhancing technologies

ENISA published the report "*Readiness analysis for the adoption and evaluation of privacy enhancing technologies - Methodology, Pilot Assessment, and Continuity Plan*" in December 2015, which is WPK 3.3´s D1. The report is first and foremost intended for Data Protection Authorities (DPAs), but also offers valuable input for networks (in particular IPEN[1]), data controllers and data processors and developers of IT products, systems or services, researchers, standardisation bodies and policy makers.

The deliverable is intended to develop a methodology that can provide comparable information on the maturity of different PETs. This methodology examines the readiness of the technology as one dimension and its privacy enhancing qualities as a second dimension, and subsequently combines these results into an overall PET maturity score. The study presents a methodology to be used to develop the overall PET maturity score and tests the feasibility of this methodology through a controlled experiment called *the IRMACard pilot study* (involving five experts, one study assessor and one study observer) and the a less stringent review called *the TOR open experiment* (involving 14 participants with a relevant background). Finally, the report proposes an action plan for the continuation of this work with assessing the maturity and usefulness of available PETs.

2.1.2 Deliverable 4: State-of-the-art analysis of data protection in big data architectures

Deliverable 4 under WPK 3.3 is titled "*Privacy by design in big data - An overview of privacy enhancing technologies in the era of big data analytics*" was published by ENISA in December 2015. The specific target group for the publication is not defined in the publication (or other secondary data), and in general the report is relevant for a broad target audience – from DPAs to industry and public sector institutions working with big data.

[1] Internet Privacy Engineering Network (IPEN)

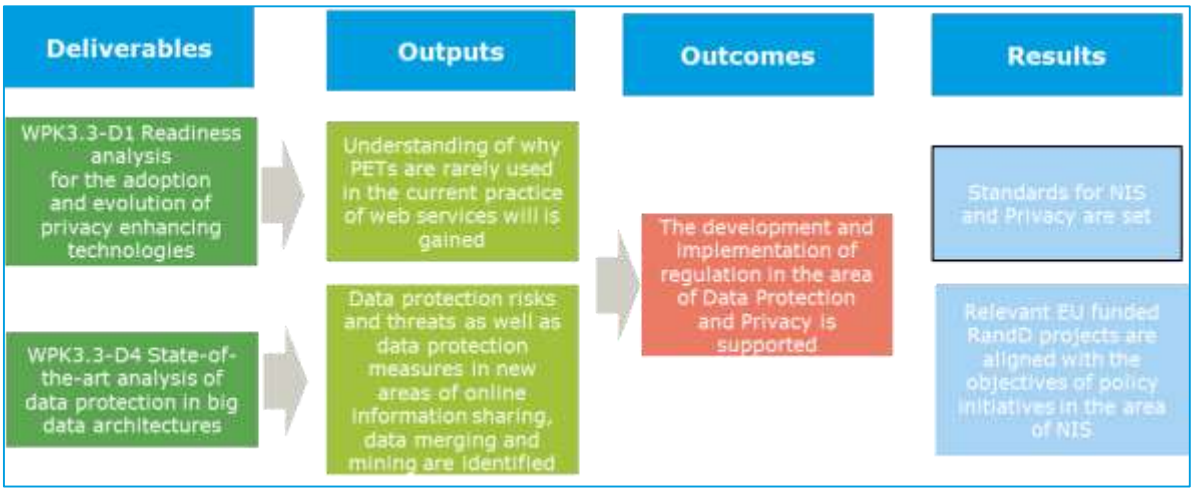
The deliverable is intended to support the development of "big data analytics with privacy" – an approach which tries to ensure that the opportunities of big data analytics can be pursued while putting limits to big data processing and integrating the appropriate data protection safeguards in the core of the analytics value chain. In order to do so, the publication presents an analysis of the proposed privacy by design strategies in the different phases of the big data value chain, and gives an overview of specific identified privacy enhancing technologies which look promising. Finally, the publication puts forward its conclusions and recommendations to guide further work.

2.2 Intervention logic

The figure below presents an extract of the intervention logic for Strategic Objective 3. It focusses on the two deliverables under Work Package 3.3 which are above the evaluation´s aforementioned threshold.

An intervention logic is a systematic and reasoned description of the casual links between the Agency's activities, outputs, outcomes, results and impacts. It helps to understand the objectives of the Agency as a whole and link this to its specific deliverables.

Figure 2: Intervention logic for Work Package 3.3 (deliverables over EUR 30,000)



The findings presented below have been structured according to the outputs, outcomes and results listed above in relation to the deliverables of Work Package 3.3. Making a judgement in relation to the degree of achievement of the intended outputs and outcomes of the deliverables will enable conclusions to be drawn on the extent to which ENISA is having an impact on NIS. This means that the findings of the case study can be integrated as evidence to answer the evaluation questions.

3. FINDINGS

In this chapter, we present the findings on the extent to which D1 and D4 under WPK 3.3 have reached the intended outputs, outcomes and, in combination, results as set out in the intervention logic described above.

In order to follow up on achievements of the different deliverables, ENISA sets impact indicators which are presented in the annual work programmes. [2] By the end of 2015, ENISA is on a good track to reach the aims set for WPK 3.3, as presented in Table 1[3].

Table 1: Impact indicators and achievements for WPK 3.3[4]

Impact indicators	Achievements by the end of 2015
At least 5 representatives from different MSs contributing to ENISA guidelines and best practice recommendations regarding Privacy Enhancing Technologies	• 6 EU MS representatives contributed to the report also supporting in the peer review stages.
At least 10 actors in the field validating the results of the studies	• 12 representatives of different sector actors contributed to the various peer review stages of the work.
More than 80 participants in APF'15 (researchers, policy makers and industry participants)	• APF'2015 was attended by more than 100 participants. The conference gathered increased interest.

3.1 Deliverable D1 Readiness analysis for the adoption and evaluation of privacy enhancing technologies

This section presents the case study´s findings on D1.

3.1.1 Output: Understanding of why PETs are rarely used in the current practice of web services

In total, this deliverable was downloaded 425 times worldwide between December 2015 (when it was published) and April 15th[5] 2016, of which 71% (301 downloads) were in the EU. The remaining downloads where primarily accounted for by the United States (10%), and a variety of other third-countries. While this data does not provide support that the output *has been reached* it indicates that there has been moderate interest[6] in the publication.

With regards to the downloads in the EU, the medium[7] used cannot be determined[8] in 49% of the cases, while 21 % of the downloads happen as a result of an organic search[9]. Finally, 30% of the downloads occur as a result of referral[10]. This is a high number, compared to the fact that the average referral percentage across all publications from 2014 (as part of that AWP) was 16%, thus indicating that D1 has been disseminated successfully through active referrals (rather than users finding the publication on their own). The interviews provided an explanation for the unusually high number of downloads generated by referral, namely that while the report is

[2] In the work programme and the annual activity report KIIs are linked to the WPKs but not to individual deliverables. The KIIs have been linked to the different deliverables based on documentation received from ENISA.

[3] ENISA Annual Activity Report 2015

[4] Please note that the evaluation report contains an assessment of the KIIs, and that for WPK 3.3 the KIIs were deemed fully achieved. However, the KIIs were assessed to not provide a measure of effects or impact, since they are descriptive in nature.

[5] The URL changed for the ENISA website on April 15th 2016 and therefore this date is used as a cut-off point. The evaluation which will be carried out by Ramboll next year will examine the number of downloads for the publication for the whole duration of 2016.

[6] The total number of downloads is deemed low since compared to the preliminary data on downloads from 2014 (see Annex B to the final report on the evaluation of ENISA´s activities in 2014), where the lowest number of downloads (for a comparable period) was 1110).

[7] Medium refers to how users get to the page where they download the publications.

[8] In a high number of cases Google Analytics cannot determine the referrer who brought the users to the page where he/she downloaded an ENISA publication. Thus, this medium, called "none" in the dataset, does not provide explanatory power in determining how users found the publication, since it can cover a variety of instances, including the two most common which are clicking a link from an email or clicking a link from a Microsoft Office or PDF document.

[9] Organic traffic is all the traffic that comes from unpaid sources on search engines like Google, Yahoo and Bing.

[10] "Referral" means that the recipient has arrived to the publication by clicking on a link on another website/email.

public, it can be accessed mainly through a link on ENISA´s website, since it has not been disseminated broadly (according to staff at ENISA). In addition, this means that there has been limited access to and awareness of the document and as such explains the low number of total downloads[11]. One interviewee specifically underlined that the visibility of this document was too low, suggesting that many interested stakeholders may not be aware of it.

Digging deeper into the usage of D1, interviewees (three) suggested that the report was more practical and more applicable to assessing the qualities of technologies privacy enhancing technologies (PETs) than other available publications. An interviewee highlighted that it is clear that ENISA is becoming more active in the field of PET and that the 2015 activities of the Agency exemplify this development. Three interviewees were unable to comment on the publication specifically.

Looking specifically at whether the publication has increased understanding of why PETs are rarely used in the current practices of web services (the deliverables intended output), four of the interviewees were able to confirm that this was the case. They highlighted that the publication provides new insights on the usage of PETs and what the challenges are. Two interviewees were able to provide examples, noting that the publication it useful in the short run since it provides and update on the development phase of specific technologies, thus making any shortcomings and opportunities of PETs more visible.

One of the interviewees noted that this publication needs to be updated on an annual basis, since technology changes quickly, but that the methodology (i.e. how to perform readiness analysis) can be applied on an annual basis. Another interviewee remarked that this publication is a good example of how ENISA´s publication helps stakeholders from different backgrounds "kick-start" their understanding of technological challenges and opportunities. In addition, an interviewee said that such reports can be used to identify relevant contact persons and experts in the field of PETs.

One interviewee noted that in general, it would be beneficial if ENISA developed material which could improve privacy for the domestic use of technologies. As an example, the interviewee highlighted that guidelines on blocking web-instruments would be useful to help private individuals navigate more safely on the web as well as guidelines for the industry on how to introduce privacy into the definition of a services or tool.

The remaining interviewees could not comment on whether the publication contributed to an increased understanding of why PETs are not used, or an overall increased awareness of PETs, because they were not part of the target group and had not received feedback from the target group.

3.1.2 Outcome: Support to the development and implementation of regulation in the area of Data Protection and Privacy

According to the survey, 21 respondents had made use of the publication and of these all 21 agree or strongly agree that ENISA's work, outputs and publications have supported the development and implementation of EU regulation in the area of data protection and privacy.

All interviewees agreed that ENISA´s activities in 2015 provided important support to the development and implementation of regulation in the area. At the same time, the interviewees who were able to comment on D1 found it difficult to describe the contribution which D1 in terms of what value the publication brings. At the same time, three interviewees were able to offer assessments based on more general statements. These interviewees said that the publication supported this outcome by increasing their understanding of the maturity and quality of PETs. Moreover, four interviewees explained that the publication has provided input to decision-makers by increasing their understanding of the challenges and opportunities related to readiness

[11] The total number of downloads is deemed low since compared to the preliminary data on downloads from 2014 (see Annex B to the final report on the evaluation of ENISA´s activities in 2014), where the lowest number of downloads (for a comparable period) was 1110).

assessments of PETs. One interviewee noted that D1 gives credibility to the notion that readiness assessment of technologies is important and that the use of PETs is an area in continuous development, which should be a priority. However, the low number of downloads of the publications suggests that the publication has had a limited opportunity to support the intended outcome.

In addition to the intended outcome, an unintended outcome was highlighted by the interviewees, namely that due to the credibility of ENISA, persons working with PETs have referenced and used the publication in awareness raising activities aimed at engaging with private and public stakeholders.

3.2 Deliverable D4 State-of-the-art analysis of data protection in big data architectures

3.2.1 Output: Identification of data protection risks and threats as well as data protection measures in new areas of online information sharing, data merging and mining

In total, this deliverable was downloaded 4,958 times worldwide between December 2015 (its publication date) and April 15th[12] 2016, of which 40% (2,004) of the downloads occurred in the EU. The United States accounting for 46% (2,278) of the downloads, while the remaining 14% are accounted for by many other third-counties. Seeing as this deliverable was only published in December 2015, the number of downloads already is high compared to the average download of deliverables in 2014 (which was 6,724 over a period of a minimum of 12 months). That being said, while the volume of downloads certainly testifies to the popularity and general usefulness of the deliverable, it is important to note that other factors may weigh in as well, for example a potentially large and diverse target audience. Importantly, interviewees emphasised that this publication was essential, and all interviews described privacy in big data analytics as an important topic.

In relation to the mediums used to generate EU downloads, this deliverable has nearly the same average as was found in the analysis of deliverables from 2014: For 61 % of downloads it is not possible to determine the referrer, for 23% the download occurs after an organic search and 15% after referral. However, the final 1% has been generated by social media (primarily by Twitter) and although this is a modest number, it is a higher number of views via social media than the average for 2014 deliverables (which was 0.09%). Unfortunately, the evidence available does not allow us to draw any firm conclusions on which distribution channels are more useful.

A majority of interviewees confirmed that D4 has reached the output, with one interviewee placing particular emphasis on the document´s contribution to identifying data protection risks as its main added value (rather than data protection measures). The interviewees explained that D4 achieved this output by:

- Making Privacy by Design understandable to a broader audience, explaining how to do it practice, and supporting software designers in developing solutions (mentioned by three interviewees)
- Filling the gaps in available information with state-of-the-art analysis, and providing a broader overview of potential standards than would otherwise have been possible (mentioned by two interviewees).
- Supporting implementation of Privacy by Design by granting access to strategies and promising PETs (mentioned by one interviewee)

Two interviewees noted that feedback from industry (primarily within the sectors of telecommunications and healthcare) has been positive, in particular in relation to allowing them to gage the on-going development amongst DPAs regarding anonymization requirements.

[12] The URL changed for the ENISA website on April 15th 2016 and therefore this date is used as a cut-off point. The evaluation which will be carried out by Ramboll next year will examine the number of downloads for the publication for the whole duration of 2016.

The case study suggests that a key influencing factor in this regard was the involvement of experts with both legal and technological expertise in the development of the report, which delivered a high-quality report relevant for stakeholders with different professional backgrounds.

3.2.2 Outcome: Support to the development and implementation of regulation in the area of Data Protection and Privacy

In the survey, 25 respondents confirmed that they had made use of the publication, and of these respondents, 21 agreed or strongly agreed that ENISA's work, outputs and publications have supported the development and implementation of EU regulation in the area of data protection and privacy. While it should be noted that respondents are not assessing the contribution of the publication on its own, but in connection with ENISA´s other activities, it indicates that the publication is making a contribution.

Some interviewees highlighted that ENISA´s role is not to develop legislation, but rather that the Agency adds the most value in supporting implementation of regulation. This assessment is reinforced by the overall assessment made by interviewees, where a majority argued that D4 has helped Member States prepare for the General Data Protection Regulation (GDPR), which was adopted on May 4th 2016 and which Member States will have to implement by May 25th 2018. One interviewee explained that D4 is especially relevant since it appeals to a broad audience through its accessible language and because it deals with privacy by design from a legal, political and technological angle. The quote below gives an example of how the publication has added value.

"DPA´s are naturally more involved in the work on the regulation than [work regarding] the technology, because this is their day-to-day work. But the technological side is important, and it [the report] bridges the legal principles with the technology".

In other words, the evidence shows that the publication has made a substantial contribution to helping Data Protection Authorities (DPA) understand, analyse and assess technical solutions from a legal perspective (as stressed by three interviewees in particular). This suggests that the output (described above) has helped deliver the intended outcome, and that the main emphasis has been on data protection measures. Furthermore, they assessed that the report has and will continue to be an important support to DPAs and Member States as a whole in the implementation of the GDPR. In this regard, the timing of the publication (in advance of the adoption of the GDPR) appeared to have been a positive influencing factor which has fuelled the interest and usage of the report. Two interviewees highlighted that DPAs are traditionally more reactive than proactive, meaning that they seek new knowledge once a complaint has been lodged. Referencing two Member State´s DPAs, the interviewees said that D4 has given the DPAs an opportunity to be more proactive in their approach to developing and supporting the implementation of regulations in the area.

Finally, two interviewees highlighted that they received positive feedback from industry stakeholders, in particular from the telecommunications industry. They explained that the publication was primarily relevant for them in their preparation for implementation of the GDPR.

3.3 Contribution towards expected results of the WPK as a whole

3.3.1 Setting standards for NIS and Privacy

While the evidence collected in the case study does not show that the deliverables have directly helped set standards for NIS and Privacy, the case study presents evidence which suggests that D1 and D4 have provided stakeholders with an understanding of standards for NIS and Privacy through:

- Providing examples of appropriate data protection safeguards (D4)
- Provides new insights on the usage of PETs (D1)

Thereby, the deliverables are indicated to contribute to a gradual standardisation of how PETs usefulness are assessed (D1), but mainly through helping Member States (in particular DPAs) navigate in an increasingly complex legislative environment.

3.3.2 Alignment of relevant EU funded research and development projects with the objectives of policy initiatives in the area of NIS

There was no evidence indicating that the D1 or D4 have contributed to an (improved) alignment of relevant EU funded research and development projects with the objectives of policy initiatives in the area of NIS. However, in addition to the publications, WPK 3.3 also delivered the third annual privacy forum (APF), which was highlighted by 7 interviewees as a crucial ENISA activity. They underlined the importance of the APF by stressing that private and public stakeholders have an opportunity to meet and learn from each other, thus bridging gaps in understandings of technology, legislation and policy objectives. In this regard, the case study suggested that one weakness of the APF was the low representation of academia, which was judged to be due to the fact that there are many academic conferences in the area of NIS and that academics are therefore hard to attract. If academia is well-represented at future events, this may bring more perspectives on technical and legal issues including a higher level of abstraction, according to one interviewee. Two interviewees suggested that if publications or papers were developed as part of the conference, academics would be more likely to participate, which could potentially boost ENISA´s contribution to this result.

4. CONCLUSIONS

At output level, the evidence available suggests that D1 has been used, although the number of downloads is low (425), mainly due to the fact that it has not been disseminated to a broader group of stakeholders. In combination, the data form Google Analytics, and the interviews indicate that in the output have been achieved to some extent. However, a majority of interviewees found it difficult to point to concrete examples of how the publication has contributed to an increased understanding of PETs and their usage (the deliverable´s intended output). With regard to D4, the evidence of achievements was stronger due in part to a higher volume of downloads (4958) and an overall stronger assessment made by interviewees, who highlighted that the publication has increased the access to more detailed knowledge on big data analysis with PETs.

An unintended output of WPK 3.3 was identified, namely that interviewees assessed that D4 has supported the exchange of information between public and private stakeholders, and between persons working with issues of PETs in big data analytics from either a legal or technical position. In particular, persons with a legal background and professional occupation highlighted that their understanding of the technical challenges and opportunities had improved after familiarising themselves with the analysis presented in D4. For example, an interviewee with a technical background (data science) highlighted that communication with Data Protection Officers has improved as a result of D4, and conversely an interviewee with a legal background working at a DPA, reported an increased understanding of the interplay between technology and law.

At outcome level, for D1 and D4, the survey provides evidence that the publications have indeed contributed to supporting the development and implementation of Data Protection and Privacy regulation. However, the evidence lends stronger support to the contribution of D4 than D1. This is in large part due to the fact that interviewees assessed that the publication provided concrete input to DPAs on the challenges and possibilities of an increased focus on privacy in big data analysis, which was assessed to be primarily relevant in the context of implementation (and not development) of Data Protection and Privacy regulation. For D4, the interviewees were able to provide explanations and examples of D4 has helped DPAs and private stakeholders understand, analyse and assess technical solutions from a legal or business perspective, and could confirm that this – already at an early stage- contributes positively to the implementation of the GDPR.

For both deliverables two influencing factors appear to inhibit the deliverables´ ability to achieve this outcome fully. Firstly, two interviewees noted that while ENISA is a respected source of technical expertise on PETs, the privacy and security environment is very fragmented in Europe, meaning that ENISA at times competes for readers and participants (e.g. to the APF), thus reducing the relative importance and outreach of the Agency´s activities. Secondly, national legal frameworks for Data Protection were reported to be confusing in some cases, with overlapping and outdated legislation making development and implementation of such legislation more complex in general. It is important to note that these factors are outside the control of ENISA, but that, when possible, they could be taken into account to reduce their impact on the effectiveness of ENISA activities.

Further to the unintended output described in the beginning of this chapter, the legal professionals´ improved understanding of technical issues with big data, which could be addressed by PETs, contributed to ENISA better supporting the development and implementation of Data Protection and Privacy regulation.

At result level, findings were mixed. On one hand, the deliverables are indicated to contribute to new insights on the availability and usefulness of PETs or examples of appropriate data protection safeguards, but mainly through helping Member States (in particular DPAs) navigate in an increasingly complex legislative environment (result no.1). On the other hand, there was no evidence indicating that the D1 or D4 have contributed to an (improved) alignment of relevant

EU funded research and development projects with the objectives of policy initiatives in the area of NIS (result no.2).

[Text - Do not delete the following line since it contains a section break. NOTE! Page numbers are updated on "Save" and "Print"]

APPENDIX 1
INTERVIEW GUIDE

Draft Interview Guide for case study WPK 3.3.

Interviewee	
Organisation	
Date	
Interviewer	

The interviewer will begin by introducing the evaluation, its objectives and scope. Not all questions needs to be probed, but the deliverables should be explored.

Explain that we are interested in understanding how the interviewee has experienced the WPK, in this case WPK 3.3. Explain briefly what the WPK was intended to achieve.

Remember to adjust your use of the questions if the interviewee answered the survey – check before hand, and ask the interviewee (NLOs may not have been selected through the survey but by ENISA, and may still have answered the survey)

Introductory questions

- What is your main area of work, can you briefly describe your main responsibilities?
- How long have you been working in this area?
- Please describe what activities during 2015 which you have been aware of/participated in.

Link in the intervention logic	Interview questions	Interview notes
1. Through its deliverables, WPK 3.3 supports the development and implementation of regulation in the area of data protection and privacy	**How would you describe the overall achievements of WPK 3.3[13]. when it comes to analysing the readiness the industry for the adoption and evolution of privacy technologies?** Is the picture different or similar if you look at the public and private sector?	
	How would you assess WPK 3.3. contribution to help system developers keep up with privacy enhancing technologies by providing recommendations on complex cryptographic building blocks? Can you provide an example?	
	WPK 3.3. was intended to provide a state-of-the art analysis of the data protection threats, risks and protection measures in the emerging big and open data landscape. How would you describe the WPK achievements in this regard? Did you participate in the third annual privacy forum?	

[13] The WPK terminology will only be used in cases where the interviewee is familiar with it, and in this case Unit COD2. Otherwise, "WPK 3.3." is replaced by the "the Agency" or "ENISA".

Link in the intervention logic	Interview questions	Interview notes
	Why did you (not) participate?	
2. **WPK3.3-D1:** Readiness analysis for the adoption and evolution of privacy enhancing technologies leads to increased understanding of why PETs are rarely used in the current practice of web services (*output*).	**Are you familiar with ENISA´s readiness analysis for the adoption and evolution of privacy enhancing technologies?** (i.e. the 2015 publication titled ""Readiness Analysis for the Adoption and Evolution of Privacy Enhancing Technologies. Methodology, Pilot Assessment, and Continuity Plan"=? **If yes,** could you tell me why and how you have used it? What did you learn from this publication? **Did it increase your understanding of why PETs are rarely used?)** Can you provide an example? Could something have been improved?	
3. WPK3.3-D1: Increased understanding of why PETs are rarely used in the current practice of web services (*output*) leads increased support towards the development and implementation of regulation in the area of Data Protection and Privacy (*outcome*).	[If the interviewee assesses that his/her understanding of PET usage has been increased] **In your opinion and experience, what where the effects of this increased understanding of PET usage?** **In your opinion, did it increase support towards development and implementation of regulation in the area of Data Protection and Privacy?** Can you provide an example? Could something have been improved?	
4. WPK 3.3 –D4: State-of-the-art analysis of data protection in big data architectures leads to better identification of data protection risks and threats as well as data protection measures in new areas of online information sharing, data merging and mining (*output*).	**Are you familiar with ENISA´s work on analysis of data protection in big data architectures**? (i.e. "Privacy by design in big data. An overview of privacy enhancing technologies in the era of big data analytics")? **If yes,** could you tell me why and how you have used it? What did you learn from this publication? **In your opinion, did it improve**	

Link in the intervention logic	Interview questions	Interview notes
	identification of data protection risks and threats? Has it improved data protection measures in new areas of online information sharing, data merging and mining) Can you provide an example? Could something have been improved?	
5. WPK 3.3 –D4: Improved identification of data protection risks and threats as well as data protection measures in new areas of online information sharing, data merging and mining (*output*) supports the development and implementation of regulation in the area of Data Protection and Privacy (outcome).	[If the interviewee assesses that his/her identification of data protection risks and threats has been approved and/or improved data protection measures in new areas of online information sharing, data merging and mining] **In your opinion and experience, what where the effects of this improved identification of risks, threats and/or data protection measures?** Can you provide an example? **Based on your experience, has it supported the development and implementation of regulation in the area of Data Protection and Privacy?** Could something have been improved?	

6. Do you have anything you would like to add?

Thank you very much for participating in the interview.