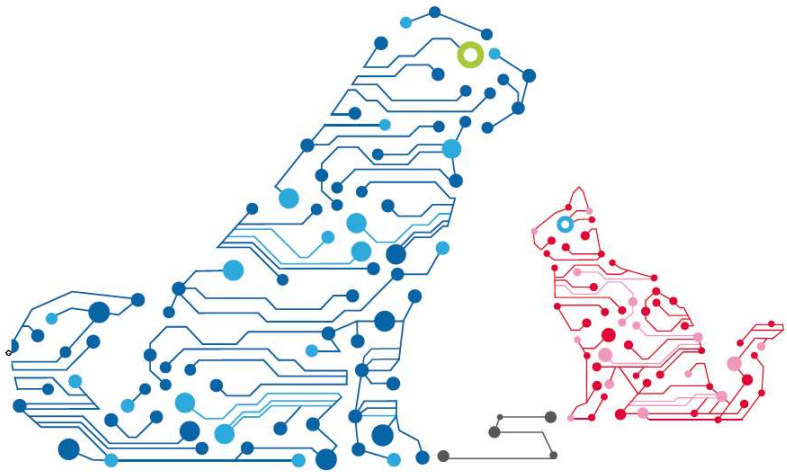


ENISA's PETs Maturity Assessment Repository

Populating the Platform

FINAL

RESTRICTED

NOVEMBER 2018

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and EU citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Contact

For queries in relation to this paper, please use isdp@enisa.europa.eu
For media enquires about this paper, please use press@enisa.europa.eu.

Table of Contents

Executive Summary 5

1. Introduction 6

1.1 Background 6

1.2 Scope and objectives 7

1.3 Outline 7

2. ENISA's PETs Maturity Assessment Repository 8

2.1 The notion of state-of-the-art in PETs 8

2.1.1 Network effect 9

2.2 The Pets Maturity Assessment Repository 10

2.2.1 The current implementation 13

3. Approaching test users and populating the platform 14

3.1 Purpose of the proposed approach 14

3.1.1 Test aims 14

3.2 Stakeholders and test users 15

3.2.1 Test users 15
3.2.2 Approaching prospective users 16
3.2.3 Targeted Events 16

3.3 Selection Criteria PETs 16

3.3.1 Selecting test cases to test the platform software and evaluation method 16
3.3.2 Selecting PETs to populate the platform – Criteria 17
3.3.3 Selected Test Candidates 17

4. Observations from the test phase and user feedback 19

4.1 Communication strategy 19

4.2 Concept of the PETs repository 19

4.3 Design and technical aspects of the platform 19

5. Recommendations for Next Steps 21

5.1 Communication Strategy 21

5.1.1 Duration 21
5.1.2 Social networks 21
5.1.3 Dedicated events 22
5.1.4 PR expert consultancy 22

5.2 Solving usability issues 22

5.3 Distribution strategy 23

Annex A: Marketing efforts **24**

Annex B: List of projects and possible use cases **26**

Annex C: List of stakeholders **28**

Executive Summary

Despite the apparent availability of knowledge about different privacy enhancing methods, tools and technologies, it is still hard to select the most appropriate one. It is even harder to compare and justify which solution is the best for a particular problem, IT environment or user advancement level. Therefore, there is a need for standardisation and centralisation of Privacy Enhancing Technologies (PET) knowledge, as well as for a widely-accepted methodology for the evaluation of such technologies. The common adoption of a PETs maturity assessment methodology and a unified way to describe a particular PET would improve the situation significantly.

ENISA started in 2016 the development of a web application prototype, called the "PET maturity assessment online repository" (hereinafter 'PETs repository' or 'PETs platform') following the recommendations made by a comprehensive methodology for PETs developed the previous years. This platform aims at providing an IT service, which will facilitate the formation of community that is able to maintain a repository of PETs assessments and a tool that will support maturity assessment methodology by implementing a systematic collaborative process.

Therefore, this report reflects the plan to formulate such a community, which would support the establishment of the PETs repository and would help in the testing of the maturity assessment methodology and the platform itself, as well as the experiences gained during the effort.

Moreover, the report shows that, in the framework of the six-month project period and despite a specific planning towards community building, the update of the PETs repository was rather low. This was due to several reasons, including communication strategy, technical implementation, as well as the overall approach taken.

In particular, considering feedback and observations throughout the 6-month project period, we come to the following conclusions and recommendations:

- Taking into account the network effect principles, it was concluded that the initial population of such a platform will take quite a long period. It is recommended that a different framework than a project to be used to further create the community (e.g. direct engagement of specific experts in the field).
- User feedback indicated that a clear branding of the platform would improve the soft trust factors. It is recommended that a clear entity is adopted as owner of the platform or that the platform is integrated in ENISA's corporate identity.
- User feedback also indicated that design and other technical aspects might have also affected the platform's uptake. It is recommended that, if the PETs repository is to be further promoted, more effort to be put on its technical implementation and maintenance.

This report is an **internal ENISA document** that, based on the aforementioned conclusions, aims to support further decision making within ENISA with regard to the PETs repository.

1. Introduction

1.1 Background

Despite the apparent availability of knowledge about different privacy enhancing methods, tools and technologies, it is still hard to select the most appropriate one. It is even harder to compare and justify which solution is the best for a particular problem, IT environment or user advancement level. Therefore, there is a need for standardisation and centralisation of Privacy Enhancing Technologies (PET) knowledge, as well as for a widely-accepted methodology for the evaluation of such technologies. The common adoption of a PETs maturity assessment methodology and a unified way to describe a particular PET would improve the situation significantly.

For these reasons, in 2015 ENISA developed a comprehensive methodology[1] for PETs maturity assessment. Under this study, the following recommendation was made:

"A community portal should be established that is used to publish tools and their assessment results. The European Commission should facilitate the forming of the portal".

Following this recommendation, ENISA started in 2016 the development of a web application prototype, called the "PET maturity assessment online repository" (hereinafter 'PETs repository'). This work was finalised in 2017 with an updated version of the tool (a test platform is available under http://pets.enisa.europa.eu). This tool aims at providing an IT service, which will facilitate the formation of a community that is able to maintain a repository of PETs assessments and a tool that will support maturity assessment methodology by implementing a systematic collaborative process.

Following the PETs repository development and update, one of the key challenges identified is the community building around this tool. In particular, it was considered of upmost importance not only to disseminate relevant information, but also to actively engage relevant stakeholders in the use and promotion of the tool (as evaluators, PETs providers or simple users of the tool). In this way, the tool can pave the way towards establishing a reliable repository of technologies, which can also support data controllers in the adoption of technical and organisational measures, as stipulated in articles 25 and 32 of the General Data Protection Regulation (GDPR)[2].

Against this background, ENISA decided under its 2018 work-programme to continue this work and particularly focus on community building and testing of the PETs repository, in co-operation with relevant stakeholders. As ENISA is expected to provide guidance on aspects of network and information security policy in the EU, it is logical that addressing particular areas of interest in designated policy areas including privacy and data protection is a reasonable extension of its work and it meets stakeholder requirements. The expected outcome of this work is that greater understanding by means of analysis can be reached and that gaps can be identified in a way that, if shared with institutional and private stakeholders, suitable measures can be put in place. As a result, stakeholders interested in network and information security

[1] www.enisa.europa.eu/publications/pets

[2] Regulation (EU) 679/2016 of the European Parliament and of the Council of 27 April 2016 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 (General Data Protection Regulation), http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=en

measures concerning PETs, can get better control and enhance their ability to mitigate successfully the risks identified.

1.2 Scope and objectives

The project's overall scope was to promote the ENISA's PETs repository (and underlying PETs maturity assessment methodology) by:

- Engaging the privacy community into its use, and
- Providing a plan for its future enhancement and wider adoption.

In order to engage the privacy community, a list of stakeholders would form an essential part of the project, together with their engagement in the population of the PETs repository with a number of specific use cases. The final scope would be to present an updated PETs repository populated with new content.

In order to achieve the aforementioned objectives, ENISA established a direct contract with the University of Luxembourg that has proven expertise on the subject matter.

The present report aims at detailing the outcomes of the project vis ā vis the aforementioned objectives.

Note: this is an internal ENISA document that aims to support decision making within ENISA with regard to the future of the PETs repository. The document will not be published on the ENISA website.

1.3 Outline

In the remainder of this report, the proposed approach to form a PETs maturity assessment community to test ENISA's platform is further examined and analysed.

After an initial presentation of ENISA's PETs maturity assessment repository (Chapter 2), the analysis sets off with the selection criteria to determine which experts should be approached and which test cases should be used (Chapter 3). Moreover, the main outcomes of this exercise and the feedback of the approached experts is summarized (Chapter 4). A proposal for potential approaches is further suggested in a way that future work can be laid out (Chapter 5).

The report closes with a proposed roadmap that aims at providing new directions for the future of this line of work in relation to PET assessments. Parties to be involved in such work include ENISA of course, but representatives of the PETs community can also be seen as contributors thereto. The report also includes an estimate of the needed effort to accomplish the desired outcomes. Should ENISA choose to pursue this course it would be important to carefully choose its stakeholders that are willing and able to contribute further. Clearly, the strategic orientation of such an activity needs to be carefully assessed prior to any concrete action being taken within the network and information security boundaries.

2. ENISA's PETs Maturity Assessment Repository

In an effort to put the project into context, in this Chapter the legal framework and relevant requirements are first briefly sketched; then the purpose of the PETs maturity assessment concept and web platform is presented, together with its main functionalities (as developed in the context of past ENISA's projects). Since this presentation is a broad outline of the project, this report also makes available a number of relevant references for the reader new to the topic.

2.1 The notion of state-of-the-art in PETs

In its Art. 25, the GDPR mandates that controllers of data processing consider, among others, the technological state of the art when defining means for data processing and during the data processing itself. While the state of the art is also mentioned in Art. 32 on security of processing and in Recitals 78 and 83, a definition comparable to those in Art. 4 e.g. personal data or processing is missing.

Furthermore, the requirement to employ state-of- the-art technologies to protect personal data is a conditional one and it depends on the dynamics of technology and business processes in any given assessment period. Clearly, the legislator had an interest in retaining options open to accommodate improvements over time, rather than setting a deterministic level of security that would become obsolete over time. According to Art. 25 and Art. 32, state-of- the-art technologies should be balanced against the 'costs of implementation, the nature, scope, context and purposes of the processing as well as the risks [...] and severity for the rights and freedoms of natural persons' posed by the processing.

Controllers and processors in charge to ensure compliance with the GDPR have to determine which state-of- the-art solutions to consider depending on their means. This is so far a challenging task due to several factors, among them there are 1) a missing definition of what the state-of- the-art, entails 2) the unavailability of ample guidance and case law on this matter, and 3) a lack of experience, as the GDPR is a legislative instrument that only recently (25 May 2018) started applying. Moreover, with no administratively set body in charge to establish the state-of- the-art, eventually the European Court of Justice much like Courts in the MS, are likely to be asked to determine on a case-by-case basis the minimum requirements concerning the state-of- the-art. A first step in this direction would be a clear formal process to determine a state-of- the-art repository with regard to available technological solutions.

Technology, and as such the state-of- the-art, is the subject of continuous research by public and private actors and it evolves in time. As a result, compliance considering the state-of- the-art emerges as a moving target. Emerging new technology may increase the risk of data breaches throughout the life time of a product or service. For instance, the availability of faster and cheaper computing resources may allow attackers to break encryption methods, which were considered secure at a certain moment in time. To ensure a constant low risk level of data breaches, the encryption of already encrypted data must be strengthened over time considering the current state-of-the-art.

One can also expect interferences with intellectual property law and competition law. For instance, consider a state-of-the-art privacy engineering tool that is proprietary and only offered by a single vendor to competitors under abusive conditions. With a legal requirement to deploy state of the art technology, this situation can be compared to expensive patented products (e.g. pharmaceuticals providing the only cure available for certain diseases). Only in addition those competitors that are unable or unwilling to adapt to the state-of-the-art proprietary or non- proprietary privacy enhancing tool may face market or even legal risks for their practices.

To balance the efforts towards data protection and risks for data breaches, but also for the privacy risk assessment, the risk must be measured and warranted in the first place. Standardisation and privacy design patterns may simplify this difficult task. Then, even the automation of a risk assessment may be eventually feasible. Risk assessment automation would also benefit the continuous re-assessment of risks throughout the life time of a product or service.

2.1.1 Network effect

From a different standpoint, a PETs platform can be seen as leveraging on the network effect. A test user enrolling and submitting his or her sample PET product demonstrates a positive external impact. The immediate interest is to solve one's own problem, being mainly confined to seeking feedback on the PET product itself. At a secondary level however, value is equally created for other users. This value is associated with the type of feedback recorded, with the opening up of the features and/or code of the PETs tool as well as by the sheer participation in an exchange platform. This last feature gives the certainty and/or expectation of value that can be created by simply tapping into the intellectual resources of the participants, being their analytical capabilities and their interest in providing feedback. The model is not substantially different from those created in the telephone network systems; the approach follows on the footsteps of social networks that work similarly and increase in value and prominence for each member as more users enroll.

In other words, and in terms put by Metcalfe's Law [3]the number of potential connections on a network increases quadratically with the number of nodes. Expanding the number of potential connections increases the value of a network and in line with Metcalfe's Law the growth in network size will be economically beneficial.

In the platform paradigm the key components are (a) users (b) PETs submitted (c) a format of PETs that can be processed by humans, even with the support of tools. Therefore a positive value effect can be expected when there is an increase in either (a) or (b). There is need of course to meet condition (c) to facilitate reviews and assessments. It is to be expected that as the network becomes more valuable for its enrolled users then more users will join. This can be conditioned with the relative smallish size of the PET community. In any case, however the sheer increase in numbers is likely to result in positive feedback loops that can increase the value of the platform as a whole.

So far, different concepts and methodologies exist that make it possible to break down legal high-level requirements to low-level software requirements to be implemented, using for example privacy enhancing tools residing or stored in shared repositories. To this end, there is a need to further streamline, complete and ease such approaches. Without extensive guidance and ready-to-use building blocks, small and medium enterprises with no or small research and development teams may struggle to consider the state-of-the-art.

[3] Yoo, C.S., Moore's law, Metcalfe's law, and the theory of optimal interoperability, 14 Colo. Tech. L.J. 87 (2015). See, also Spulber Daniel F, Yoo, C.S., Networks in telecommunications, Cambridge University Press (2009).

2.2 The Pets Maturity Assessment Repository

To build and maintain such a repository, a broadly accepted methodology for the evaluation of PETs has been singled out as a necessary precondition. The common adoption of the PETs maturity assessment methodology and a unified way to describe a particular PET would improve the situation significantly. To this end, ENISA developed a comprehensive methodology for PETs maturity assessment[4] and developed a web application prototype, called the "PET maturity assessment online repository".[5]

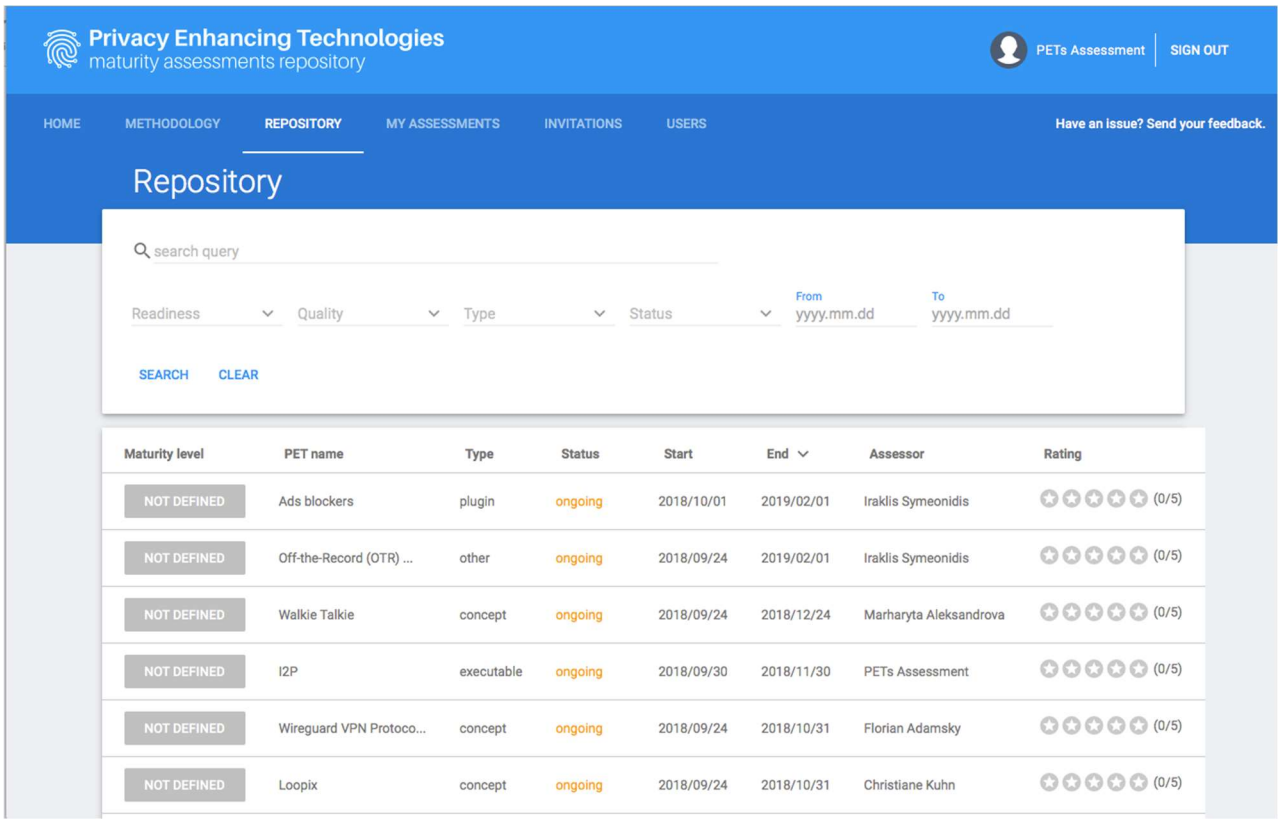


Figure 1: Snapshot of the PETs Repository

Error! Reference source not found. shows the current repository including some of the introduced test cases. For the Maturity level, a two-dimensional scale has been proposed that informs about technology readiness and privacy enhancement quality: i.e. PET maturity. We therefore determine "PET maturity" as a result calculated from a "technology readiness" and a "privacy enhancement quality" scale.

Readiness level of a PET expresses whether a PET can be deployed in practice at a large scale, or whether it can only be used within a research project to build upon to advance the state of the art in privacy protection. Readiness level indicates the amount of effort, i.e. time, money, etc., still needed to allow the PET to be used in practice with a positive cost benefit balance. We favoured the following set of readiness levels over a linear scale to ensure comprehensibility[6].

[4] https://www.enisa.europa.eu/publications/pets
[5] http://pets.enisa.europa.eu/#/repository
[6] See "Readiness Analysis for the Adoption and Evolution of PETS"(March 2016), http://pets.enisa.europa.eu/#/repository

- **Idea.** Lowest level of readiness. The PET has been proposed as an idea in an informal fashion, e.g. written as a blog post, discussed at a conference, described in a white paper or technical report.
- **Research.** The PET is a serious object of rigorous scientific study. At least one, preferably more, academic paper(s) have been published in the scientific literature, discussing the PET in detail and at least arguing its correctness and security and privacy properties.
- **Proof-of-concept.** The PET has been implemented, and can be tested for certain properties, such as computational complexity, protection properties, etc., i.e. "Running code" is available, but no actual application of the PET in practice, involving real users, exists, nor is the implementation feature complete.
- **Pilot.** The PET is or has recently been used in practice in at least a small-scale pilot application with real users. The scope of application, and the user base may have been restricted, e.g. to power users, students, etc.
- **Product.** The highest readiness level. The PET has been incorporated in one or more generally available products that have been or are being used in practice by a significant number of users. The user group is not a priori restricted by the developers.
- **Outdated.** The PET is not used anymore, e.g., because the need for the PET has faded, because it is depending on another technology that is not maintained anymore, or because there are better PETs that have superseded that PET.

The quality of a PET is not only determined by its readiness. In fact, several PETs at the same readiness level may have varying levels of quality. For this reason, nine quality characteristics, namely protection, trust assumptions, side effects, reliability, operability, performance efficiency, maintainability, transferability and scope are defined.

While each of these characteristics is relevant for a PET independent of its readiness level, the indicators that determine the score for each of the characteristics do depend on the readiness level. For example, the quality of a rolled out product depends on how well it is supported by a help desk, code updates, etc. These indicators are irrelevant for research level PETs. Here, the quality is determined by the quality of the re-search, e.g. the ranking of the venues in which the research is published.

For each of these nine characteristics, a PET can receive a score in the range {−− (very poor) − (poor) 0 (satisfactory) + (good) ++ (very good)}. The overall quality level also utilises this five-value scale, and is comprised of the nine individual scores, according to a specific quality evaluation function.

The scales for readiness and quality defined above allow us to define the real scale we are interested in: a scale for PET maturity. In fact, this overall scale is simply the combination of the readiness level superscripted by the quality level. So for example, a PET with readiness level $pilot$ and quality $+$ has an overall PET maturity level of $pilot+$. Thus, the total set of potential PET maturity values spans from $idea--$ and $idea++$ to $outdated--$ and $outdated++$. The full set of possible values is illustrated in Figure 2.

Figure 2: Overview of Possible PET Maturity Level Values

In order to introduce PETs and perform assessments, this platform needs to be populated with experts who are prepared to share their work and experience in a way that PET products improve as a result of interaction among peers. This many-to-many relationship has been thought to be powerful as much as it is capable of stimulating innovation. While learning by doing (i.e. exchanging data on PETs) is a valid expectation), learning by seeing how others work and how they reason about their own PETs is deemed to be powerful. This is likely to provide new impetus to PET tool development and slingshot the performance, quality and ability to meet regulatory requirements of PETs hosted on the platform, to higher levels. A method-driven approach provides a suitable basis to reflect formal regulatory requirements on the proposed PET tools as well as on the platform and render familiar the peer platform members with compliance requirements. This way peers become more confident on their individual abilities to build robust and compliant products that meet user expectations thus raising the overall level of performance vis-à-vis the regulatory framework in place.

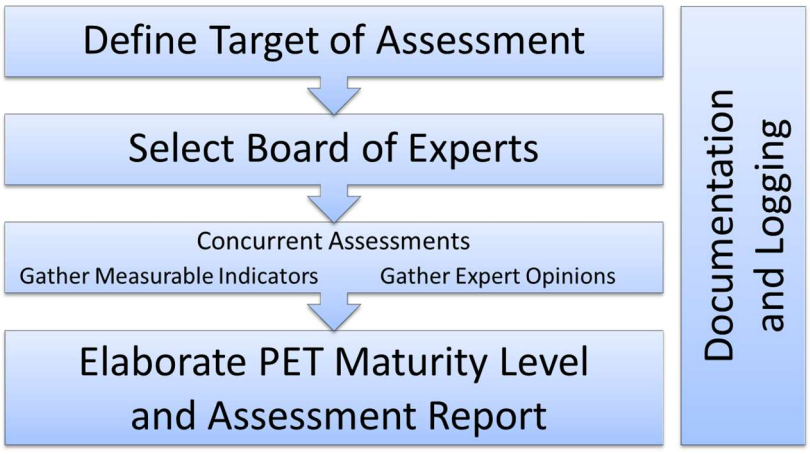


Figure 3: Overview of the assessment process

Figure 3 provides an overview of the assessment process that need to be carried out in the platform. Test users need to define targets of assessment based on products they submit for review. Test users also need to select the board of experts to provide such assessments. It goes without saying that test users are

equally expected to render themselves available to act as members of the board of experts of the platform and share their expertise with their peers.

2.2.1 The current implementation

The platform made available by ENISA provides an interface to define PETs as a target of assessment. The assessor can provide descriptions and initial sources of evidence. Furthermore, they can issue individual invitations to participants (i/e/ peers) to become members of the board of experts. The experts then are permitted to concurrently assess a PET and submit their opinion. Until then, the system supports the assessor to keep experts unaware of the intermediate results of each other. This ensures a higher level of opinion, which nevertheless can further be subjected to feedback as it is shared among all expert reviewers. Furthermore, the platform keeps full documentation and logs all interactions that allow for a high level of transparency to be enjoyed among peers.

After the individual assessments, the assessor needs to reach consensus on the PET with the support of all experts that have contributed to the assessment. The platform supports the assessor to aggregate the different expert opinions and indicates conflicts. Eventually, the consensus conclusion is published as an assessment and can be searched and consulted by the consumers of the platform, primarily the peer that has submitted the tool for assessment as well as others who may be in the future interested by a particular tool. An additional feature is that the platform can be used to keep full records of all products along with their consensus assessment reports that have been submitted over time. This feature is likely to provide an additional value point as over time progress can be analysed and benchmarked while the progress made can enhance the collective ability of PETs experts to determine the state-of-the-art.

Such a platform is likely to be seen as a contributing element to the state-of-art as it is perceived, analysed, and evaluated overtime, helping to form a technology view that is proportionate and in line with the expectations set in the legal framework as determined in the GDPR. This platform can provide the quantitative and factual basis upon which the appraisal of the state-of-art is determined; clearly the impact for legal opinion and judgement can be boosted with the successful implementation of a service based on this platform.

3. Approaching test users and populating the platform

In this Chapter, the approach followed in order to achieve the project's objectives is described. In particular, the aims, stakeholders and specific selection criteria are discussed in more detail. A list of relevant use cases for populating the platform is also presented.

3.1 Purpose of the proposed approach

3.1.1 Test aims

As described under Subsection 2.2.1, a prototype of a web platform for the proposed maturity assessment method has been implemented. This platform is currently available online[7]. Tests during the development stage have demonstrated that the platform is suitably stable for a test phase and that it can be tested with a larger, more realistic user group. It must be added here that development has been carried out while full documentation of the various stages remained a standing goal. This clearly adds to the quality of the software produced, which allows for easy tracking of actions taken and changes should particular practices be deemed to be insufficient for the shifting goals of the platform.

By populating the platform with experts and evaluations, the aims are to:

- Evaluate usability
- Understand user requirements
- Collect user feedback for the purpose of improving the implementation
- Understand market needs
- Fine tune the parameters of the approach proposed
- Allow for additional features or methods to be further integrated in the platform to render it more usable and effective.

To achieve these aims, a first step is to resolve bootstrap issues. If a community platform is populated it means that it meets user demand. If there is user demand for such a service offered by means of a platform it will be easy to attract new members and fuel the intellectual content of the platform. The critical element is to start attracting the first users on the platform. New entrants of an unknown and previously untested system are likely to influence their choices by giving consideration to perceived benefits. The dilemma is to make a proportionally larger effort while the expected positive effects are very limited in the short run and they can only pick up in the long term. As adoption costs for early users are likely to be high and the benefits are expected to be low, the platform needs to appeal to select groups of users likely to tilt their choice in favour of opting for using the platform. Hence, targeting enthusiasts, researchers and privacy advocates to overcome this mismatch seemed like a reasonable goal to pursue. In Annex C there is preliminary list of organizations that have been duly informed of the benefits and the functionality of the platform and they are expected to act as ambassadors in favor of others using the platform.

Feedback from test users has been collected through face-to-face meetings, conversations and emails. User feedback ranged from concrete feedback discussing features, usability and general feedback of the marked need of the platform. Moreover, some users have raised security concerns with regards to the

[7]Web address of the maturity assessment tool: http://pets.enisa.europa.eu/

current implementation. At this stage, it is logical to make clear that the current state of implementation of this platform does not aspire to meet commercial grade application levels of security and it merely provides a proof of concept in an effort to stimulate interest in the next phase of the feasibility assessment and gain feedback on possible shortcomings and opportunities. The results of these discussions are further summarized in Chapter 4.

Moreover, the platform has been presented at conferences and meetings to further understand Market needs. Conferences were selected opportunistically with a view to retain costs low. Conferences present an interesting forum to present and share information on this platform while seeking feedback of knowledgeable people in the field. Such parties may also act as possible target audience to populate the platform with the peers required.

Lastly, another important element was to test and fine-tune the evaluation method. The method depends on several parameters such as the evaluation criteria and their importance for the final evaluation results. For the time being, these parameters are set by educated guesses of the authors and implementers of the platform. However, they need to be fine-tuned in such a way that the evaluation results become intuitive.

3.2 Stakeholders and test users

The question of stakeholders for a platform that aims at PETs far exceeds the members of the discreet community that mostly deals with PETs from a technology and compliance point of view. Expert users can indeed benefit from an exchange platform. However, the fall out of their work and the potential of leveraging upon networks of users to improve PETs can exponentially serve and benefit all stakeholders that may have an interest in PET technologies. This potentially includes the entire internet enabled population in a specific jurisdiction.

3.2.1 Test users

It must be highlighted, that on the outset, the following user groups were identified as being key for the test users' composition:

- PETs providers: their role is to make information about PETs available within the ENISA's platform.
- Evaluators: their role is to provide maturity assessments for different PETs through the tool.
- Users: data controllers, DPAs, researchers or other interested users who can use the platform to get information about the state-of-the-art on PETs.

The above groups can be mapped to software developers, IT professionals in the field of PETs, and Regulatory bodies. In the following paragraphs, we shortly describe their use cases on the platform.

Regulatory Bodies: In Europe, national data protection authorities are appointed to implement and enforce data protection law, and to offer guidance, see GDPR chapter VI, especially article 57[8]. An up to date and maintained repository of PETs will be a resource to provide guidance with regards to state-of-the-art technical protection measures for personal data. The repository will further support DPAs to assess if measures in place are indeed proportional to the assets at stake.

[8]Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

Privacy Professionals: IT experts with a focus on privacy and data protection develop and research new protection measures. The platform will provide them with a tool to perform assessments and further understand market needs.

Software and Service Developers (IT Industry): IT experts working on new application and services that handle and operate on personal data can use the repository as a knowledge source. This will create a more transparent and competitive market of PETs. Moreover, by defining targets of assessments, IT professionals might put their ideas at challenge to demonstrate market need.

3.2.2 Approaching prospective users

In order to attract prospective test users, the platform is hosted under a subdomain of ENISA in an effort to leverage on a given community or stakeholders that have a firm interest in security and privacy as well as on the brand of a specialised EU Agency. Moreover, a leaflet describing the platform was created, which describes shortly the aim and functionality of the platform (Annex A).

For the direct and indirect communication with the stakeholders, the following means were created: the platform itself under an easy to remember address, a leaflet and 2 functional mailboxes pets@uni.lu and pets@enisa.europa.eu. Further on, some first contacts were followed up by email and calls.

Moreover, those that agreed to co-operate, especially users that introduced test cases received follow-up calls for feedback. The outcome of these follow-ups can be found in Section 4.1.

3.2.3 Targeted Events

In order to target the above listed test users, we presented the idea and platform at scientific events. The approach was mainly opportunistic, i.e. the work in this field was presented as a discussion point included in a related presentation. However, dedicated efforts were taken at the Annual Privacy Forum 2018[9], in which members of the target audience where directly approached to show "hands on" the current implementation of the tool. Further, a short presentation of the tool was presented in the IPEN workshop[10].

3.3 Selection Criteria PETs

Targets of assessment were selected in order to test the platform. In this section, we shortly describe examples of PETs that could be assessed with regards to their maturity. Given the above aims for our test, two sets of criteria to select test cases arose, i.e. for testing the platform software and evaluation method, and for populating and attracting more users to build a community.

3.3.1 Selecting test cases to test the platform software and evaluation method

In the first category the following aims should be reached:

- Ensuring code coverage, and
- Ensuring evaluation results coverage.

[9] The Annual Privacy Forum is a series of conferences organized annually across the EU that seek to bring together privacy experts from academia, policy and the private sector. ENISA is the brand owner and the main driving entity behind the Annual Privacy Forum. See also, https://2018.privacyforum.eu

[10] IPEN is a series of workshops, organised annually by the European Data Protection Supervisor, that seek to bring together privacy experts associated with public authorities, industry, academia and civil society. The scope of the IPEN workshops is to discuss relevant challenges and developments with regard to the implementation of data protection and privacy. See, https://edps.europa.eu/data-protection/our-work/ipen/ipen-privacy-engineering-workshop-2018_en

Various quality and readiness levels: PETs need to be selected for broad functionality and code coverage. Hence, for testing purposes, test candidates of possible low protection levels and technology readiness levels are needed. This leads to the need of variance in expected maturity and quality, including legacy PETs and a sort of Zero PET to reach low-quality ratings.

3.3.2 Selecting PETs to populate the platform – Criteria

Going beyond the mere software test, selected PETs need to be of a certain general interest. In this category, we summarize criteria that help to select targets of assessment, which are attractive for future users of the platform. Since adding interesting PETs will increase the utility of the platform for future users.

Diversity in privacy protection goals: The classical CIA information security protection goals, i.e. confidentiality (C), integrity (I) and availability (A), have been extended for privacy protection. Hansen et.al proposed unlinkability, transparency and intervenability as additional concepts for the construction of PETs.[11] The authors define Unlinkability as separating data and processes, transparency as adequate level of clarity in the relevant data processing and intervenability as the possibility for parties to involve in the relevant process.

The scientific PETs community until recently focused on unlikability goal as can be seen in the large number of publications with regard to anonymous communication, electronic voting, private search and private search. In order to cover all protection goals we selected the following application areas:

- Anonymous communication
- Privacy friendly access control
- Transparency tools

High maturity level: Often developers are challenged with the question which technology to use. To attract these user groups, the platform needs to provide an extensive repository of mature PETs that provide a high protection level as well as a high readiness level.

3.3.3 Selected Test Candidates

Given the above selection criteria, we selected the above candidates for evaluation (Annex B).

Fraunhofer INDUCE:[12] is a security framework for data usage control in industrial environments. It supports the fine granular implementation of a need to know principle. INDUCE is a highly consumable framework with several implementations on a large scale. This framework was selected to be evaluated with the possible outcome of a "Product".

PrivacyFlag:[13] this was selected as an EU research project produced several Prototypes and proofs of concept. The PrivacyFlag browser add on aims to support users in deciding if a webpage is trustworthy and secure. The PrivacyFlag mobile app helps end users to rate apps and public IoT implementations to assess their privacy impact. Other results help users to make better use of the anonymous communication tool TOR (EUTOR) and help to understand Website finger printing, a new technique to break anonymity in

[11] Hansen M. (2012) Top 10 Mistakes in System Design from a Privacy Perspective and Privacy Protection Goals. In: Camenisch J., Crispo B., Fischer-Hübner S., Leenes R., Russello G. (eds) Privacy and Identity Management for Life. Privacy and Identity 2011. IFIP Advances in Information and Communication Technology, vol 375. Springer, Berlin, Heidelberg

[12] https://www.iese.fraunhofer.de/en/competencies/security/ind2uce-framework.html

[13] https://privacyflag.eu

anonymous communication networks. These prototypes were selected to cover the range from research idea to pilot.

IRMA:[14] It offers privacy-friendly authentication based on attributes. This product allows the user to reveal only relevant properties for the given service. The ecosystem is grouped around mobile app on the users' phone. IRMA provides an extensive user-base in the Netherlands, but is not very much know outside of its Dutch ecosystem. Moreover, it is not clear what its future business model could be. These facts make it being an interesting test candidate for the differentiation between prototype and pilot.

I2P[15]**, TOR**[16]**, Free Proxy servers**: These 3 Protocols implement the same high-level functionality, that is anonymous communication. They should be among the test candidates to evaluate the capabilities to compare PETs using the platform. It is expected that TOR and I2P differ largely in their market readiness. At the same time, Free Proxy services most likely will contrast to the other two with regard to their quality score.

[14] https://privacybydesign.foundation/irma/
[15] https://geti2p.net/en/
[16] https://www.torproject.org

4. Observations from the test phase and user feedback

The community-building phase of the project was initiated in June 2018 and lasted until September 2018. Despite the definition of a specific approach (Chapter 3), the uptake on the platform has been generally slow. Indeed, in October 2018 only a few use cases were integrated in the platform, while the user community has not been significantly active. To this end, we collected feedback by unstructured (phone) interviews or received feedback by mail. Almost all contacted potential test users did give their feedback in various levels of detail.

In the following Sections, we describe the main observations with regard to the low uptake, as well as relevant user feedback.

4.1 Communication strategy

As a first observation, focusing only on directly targeting potential test users turned out to be very time consuming and we experienced a relatively low response rate.

Especially considering the expectation that testers and future users will contribute without monetary compensation, the advertising time of 4 month was rather short. Many of the contacted experts did in fact promise to contribute but were asking for a time-frame of 3 to 6 month. This can be seen also in the uptake for the first contributions: several experts from the first round of contact did indeed contribute after a reminder in the last round.

4.2 Concept of the PETs repository

Primed users were always convinced that a community driven tool that helps to create and maintain a state of the art repository of PETs is very much needed and helpful. See, e.g. the report of Privacy Engineering Research and the GDPR Workshop: A Trans-Atlantic Initiative[17]. However, the present implementation received some critique.

A very common feedback was that the website does not clearly address the target audience. The explanation should not be hidden in a PDF, but needs to be on the webpage as a short "about" page. The challenge will be to welcome the target audiences. Maybe with a welcome page including a first self-assessment, dividing the three main target groups. Another remark often made to this end was "If I would have stumbled upon it on the web without your intervention, I would have clicked away in seconds."

Even users that did not stumble upon this first impression struggled with the concept of expert and assessor. They found it hard to distinguish the two concepts. This contributed also to the impression that introducing assessments is time consuming (noted by 2 experts that opted not to contribute).

4.3 Design and technical aspects of the platform

Another aspect that was relevant to low uptake was the design and other technical aspects of the PETs repository.

To start with, many users were surprised that the platform was not clearly branded. Often the question was raised why it was not ENISA or EU branded. Apparently, that would have had a major impact on the general trust in the service. Some users recognized the Google Material Design, which lowered their trust

[17] https://dtai.cs.kuleuven.be/events/privacy-engineering-research-and-gdpr-workshop-trans-atlantic-initiative

in the service. The tabular structure was another design issue. Many users did not notice without help that the next step could be performed by clicking on the next the tab. Here, a wizard like GUI would have helped, according to these users.

Moreover, several users were taking issue at the fact that the web service is unprotected (no use of TLS). Most test users accepted the explanation that the platform is a prototype with clear aims what to test. However, at least one expert expressed that these concerns made them not to contribute further. Among these critical users, someone also did some testing of the registration form and seems to be credibly sure that it is not hardened against SQL-injection attacks.

It should be noted, however, that ENISA had made clear in all communications with experts that this platform was only a test bed (so as to start the whole project) and not the final tool, which would clearly be adequately protected and secured.

5. Recommendations for Next Steps

The experience of the 6 months attempt to promote and populate an existing community platform for that matter taught us that a community approach turns out to be hard to implement and that design and implementation do affect the trust in such a tool, even for a test.

Moreover, we believe that we observed a reverse network effect. That is for early adapters a community approach displays little to no utility, but rather high efforts in understanding how to use the platform, which inhibits the adoption.

To overcome these two aspects, we recommend to leverage existing communities, implement a social media strategy and create tangible advertisement material. Next to this, the feedback of test users indicates further that the security but also the branding of the platform would be important aspects to build further trust.

In this section, we map out future activities and recommend future steps. We enrich this road map with rough cost estimations in terms of person month and durations.

5.1 Communication Strategy

As already mentioned, it has been determined that focusing only on directly targeting potential test users was a very time consuming exercise, which also led to a low response rate.

5.1.1 Duration

A longer duration period could probably enhance user contribution, taking into consideration that the short time frame was one of the reasons for slow uptake. Since we still believe that direct contact with relevant test users and early adapters is key, it is **recommended that ENISA could set up a permanent contact point** for these relevant key contacts.

Needed effort. Running such a permanent contact point would need some sort of regular newsletter (quarterly) to remind the community of the platform. The effort in person month is highly depending on the success of the platform. Given that content for a newsletter can be provided by related efforts, we would expect 1 day/ per newsletter entry.

5.1.2 Social networks

Beside the maintenance of direct contacts, we further believe that platform owner **and stakeholders are recommended to leverage the existing social networks for a viral marketing approach**. For a concrete effort estimation see section 5.1.4.

Moreover, **stakeholders are recommended to research opportunities with platforms like SourceForge**[18] i.e. a platform that supports the open source community to develop and distribute software. Open questions with regard to them: can a maturity assessment be integrated in the platform, and can the community be motivated to support systematic maturity assessments. Moreover, the success of this effort depends on the usability and utility of the platform (see section 5.2)

[18] https://sourceforge.net

Needed effort. It is hard to estimate how much effort the first contact with such platforms is. After first contact, the effort should be marginal.

5.1.3 Dedicated events

For a future version, **ENISA could organize a "Road Show"** to promote the platform. For this, 5 to 10 relevant events should be selected to be present with a booth and advertisement material.

Needed effort. Given existing advertisement material, per event 1 person week is needed to prepare such a booth (contacting event, trip, logistics). Further, the financial effort w.r.t. to registration and sponsorship fees can vary largely. Typical sponsorships for small events start at €2,000. Furthermore, several events close to the community might be willing to give away free space. However, high-end events might cost €10,000.

5.1.4 PR expert consultancy

Expert consultancy in PR is recommended for both before sketched ideas.

Social media channels: In order to reach out to a larger community social media channels need to be created and maintained. For the target audience, focus should be on professional communities such as LinkedIn[19] and research focused communities such as ResearchGate[20]. Moreover, twitter could be used for communication to the general public.

Advertisement material: In order to support the "Road Show" physical advertisement material needs to be created. Here a one-page folder and a poster should be the first step. Moreover, short presentations with voice over on how to use the platform from the three typical rolls should be created as short advertisement videos. According to the above sketched feedback, it is important to stress, that these material should create a common graphical identity for the platform and its advertisement.

Needed Effort: Creating a LinkedIn topical page and a ResearchGate project can be done with the existing material in a short period, e.g., 1 person week. Note the existence of these pages only is valuable if they are maintained.

Creating a graphical identity for the project is most likely a rather big effort. However, synergies might emerge if ENISA takes the decision to take the platform under the umbrella of their cooperated identity.

5.2 Solving usability issues

As already mentioned, another aspect that might have led to a suboptimal performance is the current look and feel and usability of the PETs maturity assessment platform.

A frequent remark was the stale design and the lack of branding. Given an exciting corporate identity or a graphical identity for the publication from above, the existing platform needs to be modified to implement it. Moreover, this will also improve the perceived trust in the platform.

Needed Effort: An update of the current look and feel should be possible in a rather short time, i.e. two to three person-month. However, an accurate estimation needs an assessment of the current source base.

[19] https://www.linkedin.com/
[20] https://www.researchgate.net

Improving security and security hardening of the platform is another parameter that should be considered. This requirement is of course essential if the platform goes in production, but, as users indicated, it may play an important role also in the test phase.

Needed Effort: Implementing basic measures such as TLS and encryption of the user database should be easy. However, the maintenance of an acceptable security level including hardening of the system against injection attacks will become a continuous effort. It is very hard to estimate an expected effort without an analysis of the existing code bas. We estimate 1 person month for this analysis.

Besides performing the above improvements to the existing code base of the platform, it might be worth of investigating to use as starting point an implementation of another existing platform that implements support for a peer review process.

5.3 Distribution strategy

In the retro perspective, the slow uptake needs to be interpreted as a reverse network effect, i.e. since a community platform becomes exponentially more attractive in relation to the number of active users; a platform with little or no users has very low utility for its first adapters. This also explains the odd situation that many experts in the PETs and data protection community indeed expressed their interest in the project, but in the end where not among the early adapters.

Our distribution strategy was to this end not fit for the purpose. Relying only on the platform itself and promotion during conferences to some extend hindered the spread. Moreover, relying only on a specific contractor proved to have certain limitations in terms of community building. An alternative approach could be to directly engage specific key stakeholders (e.g. from the list in Annex C), who can immediately act as users of the PETs platform and further disseminate it to their communities.

Furthermore, a future effort needs to interlink the platform with social networks. However, this can leverage the existing general-purpose networks like Facebook, Twitter or Linked in. Moreover, it needs to be explored if and how it could be possible to interlink or even integrate such a platform with existing open source platforms such as source forge.

Annex A: Marketing efforts

A leaflet was created to distribute it during events.

pets.enisa.europa.eu

WHY?

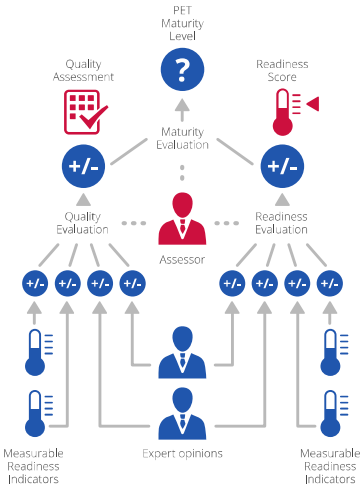
While privacy enhancing methods, tools and technologies have been broadly available, it is still challenging to make the right choices for a given purpose. Comparing solutions to match criteria for a particular IT environment or user level is an emerging area. There is a need for a repository of Privacy Enhancing Technologies (PETs) and guidelines on how to use them.

WHAT?

A repository and a standardized methodology for the evaluation of PETs could improve the situation.

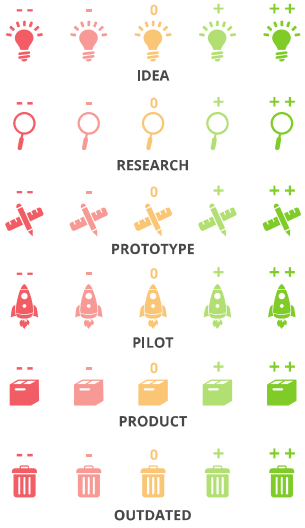
HOW?

ENISA has presented a comprehensive methodology for PET maturity assessment and developed a web application prototype, namely "PET maturity assessment online repository" (PETs repository). At this stage, this platform needs to be populated with experts and evaluations for testing.



THE ENISA METHODOLOGY

We propose a two-dimensional assessment that informs about technology readiness and privacy enhancement quality: the so-called PET maturity. For more information, please see: https://www.enisa.europa.eu/publications/pets



THE CURRENT IMPLEMENTATION

The PETs repository provides an interface to define PETs as target of assessment. The assessors can provide descriptions and initial sources of information. Further, they can invite a board of experts. The experts may concurrently assess the PET and submit their opinion. Following the individual assessments, the assessor needs to reach consensus with the experts.

Annex B: List of projects and possible use cases

PROJECT ACRONYM	PROJECT	FUNDING AGENCY	COORDINATOR	PROJECT DURATION	WEBPAGE
TAS3	Trusted Architecture for Securely Shared Services	EU FP7	KUL	31/12/2007-30/12/2011	http://www.tas3.eu
PrimeLife	PrimeLife	EU FP7	IBM	29/02/2008-27/02/2011	http://primelife.ercim.eu
PrivacyOS	Privacy OS	CIP		31/05/2008-30/05/2010	
SPION	Security and Privacy for Online Social Networks	IWT	KUL	27/12/2012-30/12/2014	
PRISMACLOUD	PRIvacy & Security MAintaining Services in the CLOUD	H2020	AIT AUSTRIAN INSTITUTE OF TECHNOLOGY	01/2/201-31/7/2018	https://prismacloud.eu
PrivacyFlag		H2020	OTE	01/5/2015-01/05/2018	https://privacyflag.eu
SAINT		H2020	NCSR "Demokritos"	01/5/2017-30/4/2019	https://project-saint.eu
Credential	Secure Cloud Identity Wallet	H2020	AIT AUSTRIAN INSTITUTE OF TECHNOLOGY	01/10/2015-30/9/2018	https://credential.eu
SUNFISCH	SecUre iNFormatIon SHaring in federated heterogeneous private clouds	H2020	MINISTERO DELL'ECONOMIA E DELLE FINANZE	01/1/2015-31/12/2017	http://www.sunfishproject.eu
ECRYPT-CSA	European Coordination and Support Action in Cryptology	H2020	KATHOLIEKE UNIVERSITEIT LEUVEN	1/3/2015-28/2/2018	http://www.ecrypt.eu.org

PRIPARE	PReparing Industry to Privacy-by-design by supporting its Application in REsearch	FP7	TRIALOG	01/10/2013–30/09/2015	http://pripareproject.eu
TYPES	TYPES (Towards transparency and privacy in the online advertising business)	H2020	FUNDACIO BARCELONA MEDIA	1//05/2015-31/10/2017	http://www.types-project.eu
DECODE	Decentralised Citizens Owned Data Ecosystem	H2020	INSTITUT MUNICIPAL D'INFORMATICA DE BARCELONA	2016-12-01 to 2019-12-31	https://decodeproject.eu
SurPRISE	Surveillance, Privacy and Security	FP7	OESTERREICHISCHE AKADEMIE DER WISSENSCHAFTEN	01/2/2012-31/1/2015	http://surprise-project.eu
VisiOn	Visual Privacy Management in User Centric Open Environments	H2020	BUSINESS-E SPA	1/7/2015-30//6/2017	http://www.visioneuproject.eu
Operando	Online Privacy Enforcement, Rights Assurance and Optimization	H2020	OXFORD COMPUTER CONSULTANTS LIMITED	01/5/2015-30/4/2018	https://www.operando.eu/servizi/notizie/ notizie_homepage.aspx
Panoramix	Privacy and Accountability in Networks via Optimized Randomized Mix-nets	H2020	THE UNIVERSITY OF EDINBURGH	01/9/2015-31/1/2019	http://www.panoramix-project.eu/
SafeCloud	Secure and Resilient Cloud Architecture	H2020	INESC TEC - INSTITUTO DE ENGENHARIA DE SISTEMAS E COMPUTADORES	01/9/2015-31//8/2018	https://www.safecloud-project.eu

Annex C: List of stakeholders

	ORGANIZATION
Industry	Jolla
	Qwant
	Fsecure
	Fraunhofer iese
	Fraunhofer sit
	Fsecure
Regulatory body	EDPS
	ULD (Unabhängige Landeszentrum für Datenschutz)
	FICORA
	Cybersecurity Center NL
NGO	Humboldt Institute for Internet and Society (HIIG)
	EastWest Institute (*EWI*)
Academia	University of Luxemburg
	KUL
	Technische Universität Dresden (TUD)
	TU Darmstadt
	Radboud University Nijmegen (RU)
	UC
	Uni Hamburg
	Technical University of Madrid (*UPM*, Universidad Politécnica de Madrid)
EU Project	
	PrivacyFlag

ENISA

European Union Agency for Network
and Information Security
1 Vasilissis Sofias
Marousi 151 24, Attiki, Greece

Heraklion Office

Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

1 Vasilissis Sofias Str, Maroussi 151 24, Attiki, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu