COVER PAGE

Cityzen Privacy

List of participants

Participant No	Participant organisation name	Country
1 (Coordinator)		
2		
3		

Contents

1 Excellence

1.1 Objectives

Citizen Privacy project proposes a solution to protect individuals' privacy by default while empowering the users to set the desired level of privacy, based on a simple to understand visualisation of the privacy level, giving them control over how their data will be used by service providers (including public authorities), and making it easier for them to verify both whether their online rights are respected and if they get a reasonable bargain.

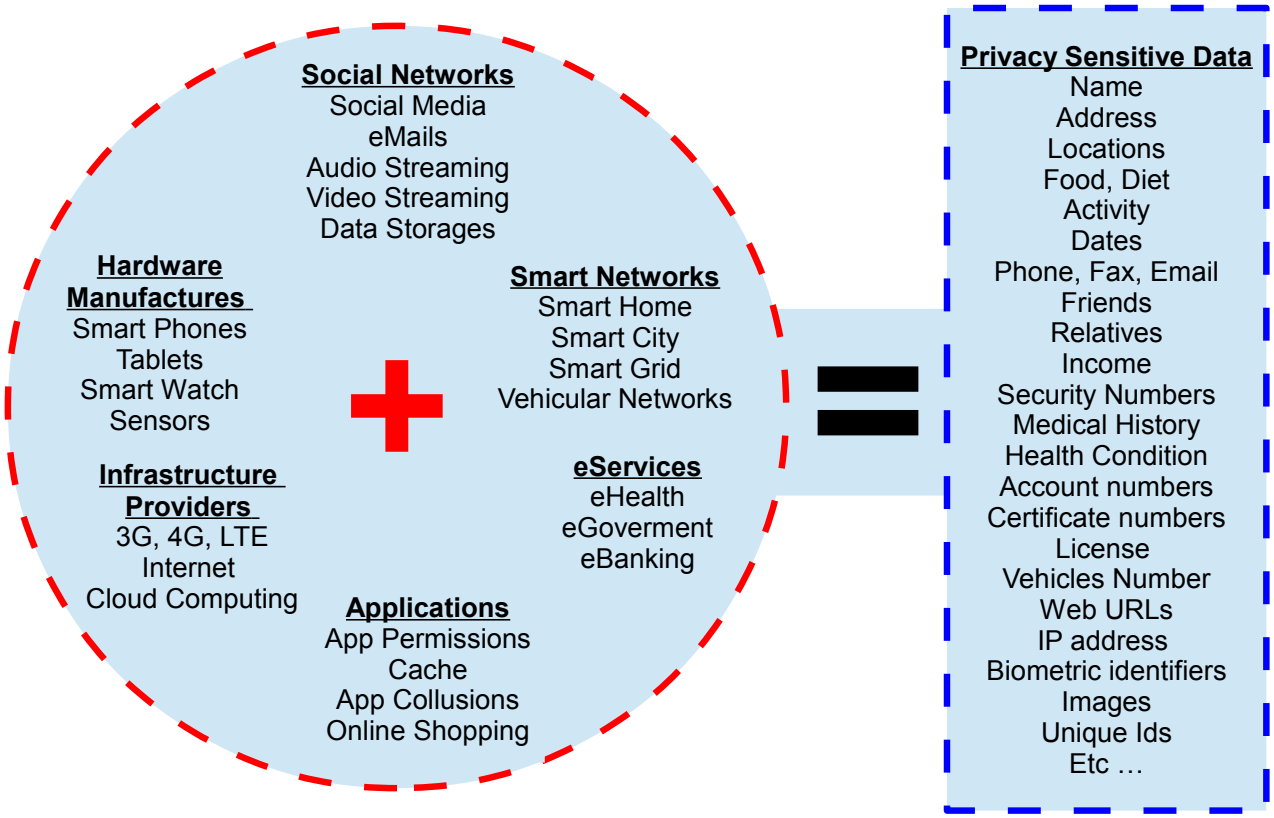

Figure 1: Citizen-centric approach is needed to cope with the increasing number of sources collecting privacy sensitive information.

The number of connected devices have exceeded the world population. Homes are now 'smart' homes where various sensors monitor health care, energy utilisation, and security. Recent trend of crowd sourcing enables cities to become 'smart' cities. This trend let many service providers to collect enormous amount of individual and organisation data which are stored in distributed databases. The amount of information in the planet doubles every 20 months and the size and number of the databases are increasing even faster. However, users don't have control over their data once it is passed to the service providers. They have little knowledge about who possess their data and how they use the data. Hence, users are reluctant to disclose the data or provide false information instead. This trend negatively impacts both the service providers and users. In order to develop the confidence level to the users, several new components must be incorporated within current Internet usage. First of all is privacy compliance verification. In EU, privacy of personal data is protected by Data Protection Directive. However, at present, there is no way for the users to validate the service provider's privacy compliance, in particularly users do not know whether the particular service provider comply with EU laws or not. Even if the service provider complies, users must be able to decide the compliance level of the service provider before release their sensitive data. Second, a trusted platform at the service provider's end to host users' sensitive data. The trusted platform allows the

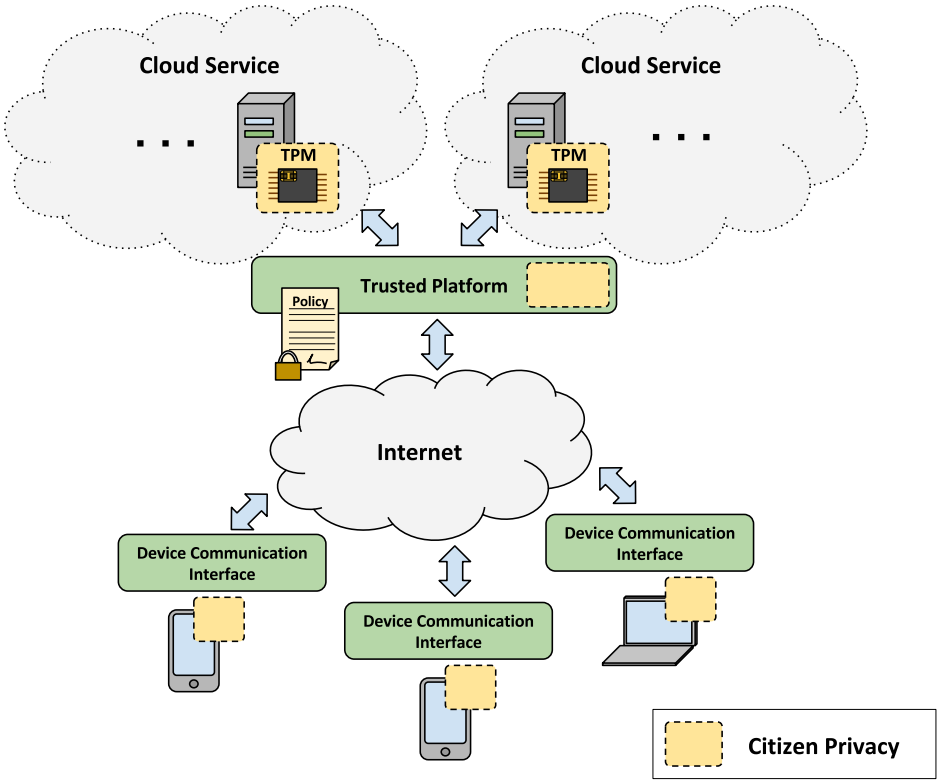

Figure 2: High-level system model

service providers to get only certain information about the data. For example, if user's date of birth stored in the trusted platform then if service provider wants to use the user's date of birth, then he can query the trusted platform to find the range of age instead of the actual date of birth. Hence, user should be able to decide what information must be stored in trusted platform before releasing the data.

Third is a privacy trust model. Even though the service providers comply with privacy legislations, the behaviour of the service provider may change over a period. The ideal way to evaluate the privacy compliance is to use the feedback of users who already doing business with the service providers. Each user can rate their experience with the service providers in terms of privacy. For example, users can poorly rate the service provider if the service provider doesn't use HTTPS secure communication technique or if they poorly maintained the users' data. Finally, a virtual interface for the users to set their privacy preferences. This interface must be convenient for the users to use in terms of defining their own preferences. Each user is unique and they require a convenient way to customise her privacy requirement. In general, female users consider their age as highly sensitive data while male users consider their annual income as their highly sensitive information. This interface could be used by the user anywhere and at any time using their any devices. Let us explain implementation and interoperability of these components below.

In this project, we build a user-centric privacy model using the above mentioned components on top of the current Internet architecture. We intend to develop user-centric privacy layer comprising virtual interface at the user end, trusted platform at the service providers, trust model and privacy compliance validation. We will develop policy to define which attributes are sensitive and which are not on individual basis. This policy will be incorporated within users' virtual interface whereby each user can set their preferences. For example, a service provider requires particular data but the data is highly sensitive for the user. In this scenario, the policy supports the users in terms benefiting from the service without violating the user preferences. In this case, the policy should say that the sensitive data must be stored within the service provider's trusted platform.

We will develop trust model to evaluate trustworthiness of the service provider in the forms of reliability and reputation by taking into account the credibility of the feedback provider. The trustworthiness of each user, computed based on the trust model, will be incorporated within the virtual interface. We will develop policy by accommodating the trust model whereby the user can have a set of options when the trust level of the service provider is less than the user's preferences. We will develop set of risk mitigation strategies and

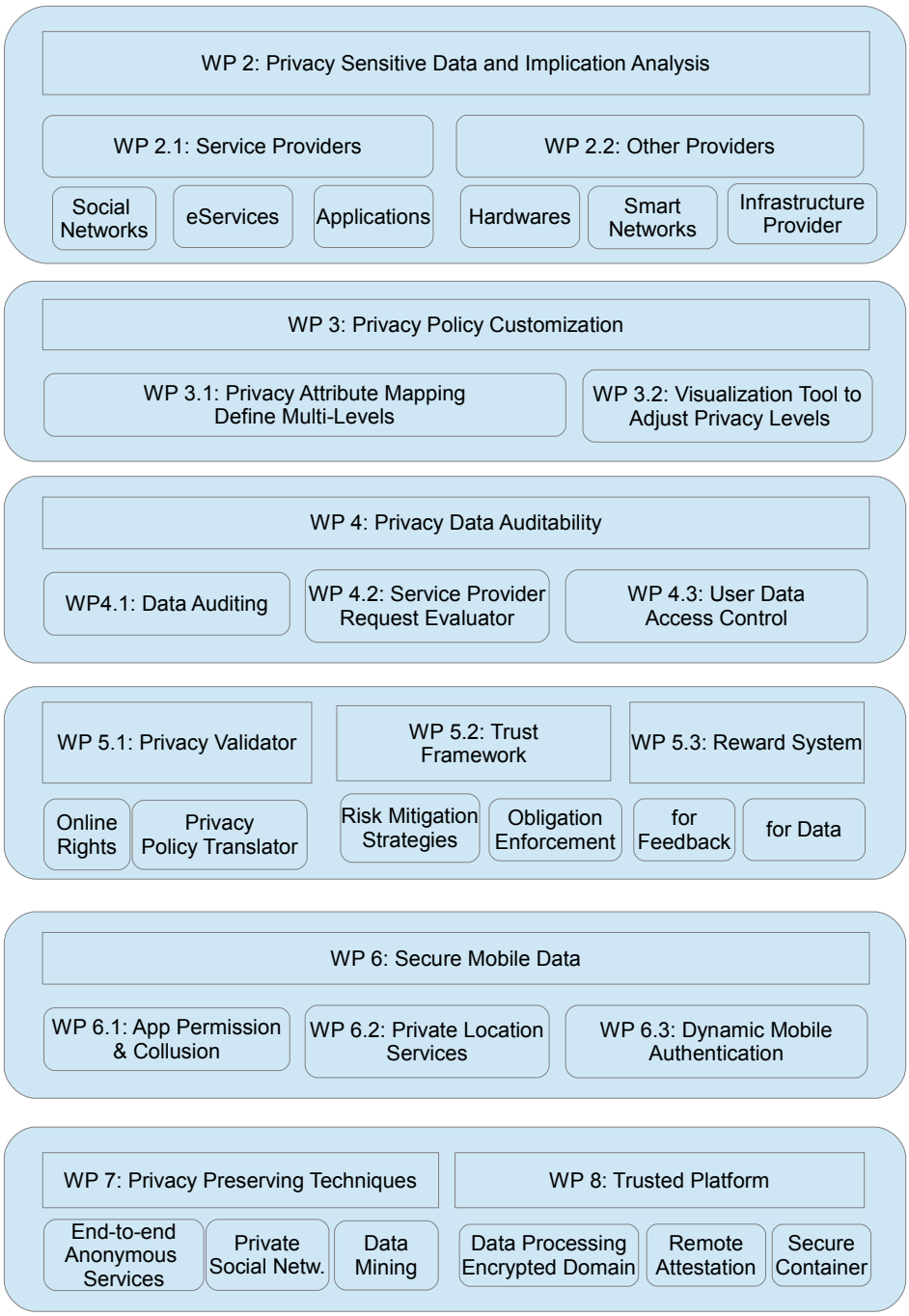

Figure 3: Work package Structure.

risk intervals when the required trust level of the service provider just below the user's preferences. When the trustworthiness of the service provider is just below the user's preference and user badly requires the service then user defines obligations for different risk level. Hence, the service provider must satisfy the obligation after receiving the data; otherwise the service provider will be rated as poor by the user. Hence, collectively this trust model enhances the users' control over their data. Since the data traffic from the mobile devices are exponentially increasing, preserving the privacy of users' spatial-temporal data from mobile operators, are cloud providers is equally important as the privacy of the data. Mobile users' spatial-temporal privacy can be achieved if set of users collaborate using privacy models such as k-anonymity. User can set the level privacy required based on the number of active proximity users in mix zones. We will

explore multi-dimensional privacy models where the spatial-temporal data of both the sender and receiver will be protected from the operators during the communications.

In service providers' perspective, their profit based on the users data. They collect users' data by providing free services. The above mentioned trust model increase the confidence level to the users to provide true data which must increase the service provider profit. In general, service providers use data mining techniques to obtain hidden patterns within users' data. When we imposed trusted platform to store sensitive information, then the data become unstructured and difficult to do the data mining. The data within the trusted platform is protected by encryption while the data outside the trusted platform is not encrypted. Moreover this will depend on users' preference. This will impact the service providers' profits which indirectly affect the service they provide to the users.

On the other hand, the collected data are being used in isolation by individual service provider which substantially reduces the distributed knowledge discovery. For example, energy companies' process energy-utilisation-data collected from households to maximise their profit but they are reluctant to share the data with environmental agencies. However, if these organisations can share the data in a privacy preserving manner then it is possible to protect the environment while maximising the profits. On the other hand banks and financial institutions never share data about malware attacks and data loss to their competitors as this can damage their reputation. Sharing of this type of cyber-attack data can help to infer common attack patterns among the organisations to develop more robust security solutions. Mobile service providers who collect individual physical activities and eating habits never share that data with healthcare authorities. If this data is shared then it is possible to identify potential health problems at an early stage. Privacy and security concerns, reputation and business competition among organisations are the possible root causes for not sharing the sensitive data.

In this project, we will develop privacy-preserving data mining technique to mine the data from unstructured and distributed data bases. The project will aim to develop privacy-preserving models based on clustering, dependency modelling, classification, regression, and graph similarity techniques using various combined cryptographic and randomisation primitives such as oblivious randomisation, polynomial evaluation, homomorphic encryption, and multi-party computation. These privacy-preserving algorithms could be exploited jointly and efficiently among service providers to reveal 'hidden intelligence' without violating the data privacy. Privacy clustering and graph similarity techniques could reveal hidden patterns between several events in a spatio-temporal domain. These patterns could be exploited to detect anomalies which can help to identify emerging new patterns.

The service providers involved in collaboration are mutually untrusted parties and they can deviate from the standard protocol. In order to profile behaviours of service providers involved in performing a joint data mining activity, privacy-preserving incentive models based on the Vickrey-Clarke-Groves model in game theory will be developed. This will detect rouge service providers who are failing to follow the agreed terms and conditions of the data usage and sharing, and hence identify colluding service providers who collaborate with each other to learn others data. However, the incentive model rewards the service providers who collaborate genuinely with new knowledge and inference. These algorithms could adaptively and efficiently changes strategies in order to stabilise the intelligence inference task irrespective of the activities of selfish service providers.

The generic objectives can be broken down in specific objectives targeting various stakeholders (see Table 1.1).

Stakeholder	**Objectives**	**Specific Objectives**	**WP**
Users	Empower users to manage their own privacy setting in user friendly way	Develop privacy policies to define different levels of privacy for individuals	WP1 (M), WP2 (D)
		Investigate various graphical user interface which is very effective in terms of defining users own privacy expectation	

		Introduce new user friendly tools to validate the compliance of privacy standards by the service provider	
Online Service Provider	Provide services to users without violating users privacy	Develop a trusted platform to store users attributes where service provider can only make sanitised queries	WP2 (D), WP4 (C)
		Implement a privacy-preserving feedback system to evaluate the trust level of the service providers	
		Implement a tool to enforce the users obligation requirements and risk mitigation strategies within trusted platform	
Infrastructure provider	Improve the quality of service without inferring the user activity	Implement end-to-end anonymous protocols to protect active and passive eavesdropping by infrastructure providers such as mobile operator and cloud provider	WP3 (P)
Third Parties	Making the anonimized user data available for sale without violating user privacy	Develop a strategy to balance the free service provided by service providers against the privacy requirements of user	WP4 (C), WP1 (M)
		Implement privacy-preserving data mining tools to infer patterns from unstructured data in distributed environment	
		Implement incentive models to reward and punish the parties involved in the distributed data mining process.	

1.2 Relation to the work program

Challenges	**Contribution of the Project**

Many online users are reluctant to disclose personal information online because of privacy concerns. Personal data has become an economic asset, but it is not the owners, i.e. the users, that control or monetise it. This is in the hands of the service providers whose business case often includes the use of data they collect (e.g. social networks, search engines, online retailers, and cloud hosting services).	Citizen Privacy project aims to provide a usable and transparent way for users to securely control their private information. Each user will be able to define different privacy levels, that will be guaranteed by a trusted platform. Citizen Privacy will allow users to fully trust any cloud service, providing guarantees for a confident interaction with any 3rd party service, as well as service providers to keep their business model unchanged. Moreover, Citizen Privacy will contribute providing a way for users to derive benefits from the data collection, for example acquiring credits that they can use on the same service, or for other services.
Data protection and privacy frameworks in Member States and Associated Countries need to be implemented in a transparent and user-friendly way to help users understand how their personal data might be used, including the economic value of their data. Such knowledge will enable them to exercise choice and know and assert their rights. As the economic value of their data is not known to the average user, they are not able to evaluate the value of their data relative to the value they assign to a "free" service. Moreover, the users have no control over what happens with their data, e.g. they cannot verify the data is not passed on to 3rd parties. This situation may influence individuals notion of privacy which may be perceived as a non-valuable asset.	The introduction of a Third-party trusted component will guarantee that the service provider will treat the collected data accordingly to the policy specified by the users. The built-in TPM component on the service provider servers will allow the certification of the code that will handle the data, this way preventing them to share sensitive data with other 3rd party services. Moreover, an estimate of the economic value of user's data will be provided to the user, that in this way will have a more comprehensive knowledge about the service he/she is using, and an effective perception of the value of his/her personal data. This process will be done automatically, thus in a completely transparent and usable way for the end user.
Data protection principles need to be visibly respected for the delivery of personalised public services, to increase trust in public administrations. Transparency is particularly important in an open government context, where personal data may be shared between different departments and administrations or across borders and where third parties can engage in the creation and delivery of personalised services for citizens and businesses.	Novel techniques will be developed in order to guarantee at the same time the privacy settings specified by the user, and the possibility for authorised (thus honest) 3rd party services to build new services, personalised for each user. Citizen Privacy will not disrupt the current business model of web services, but will allow the creation of an improved business model, that will encourage the usage of services thanks to new privacy guarantees. At any time the user will be able to verify the respect of the privacy policy he/she specified querying the Trusted Platform service.

The focus is on the demonstration of solutions to protect individuals' privacy by default while empowering the users to set the desired level of privacy, based on a simple to understand visualisation of the privacy level, giving them control over how their data will be used by service providers (including public authorities), and making it easier for them to verify both whether their online rights are respected and if they get a reasonable bargain. The activities may also cover tools facilitating the information of individuals about the processing of their personal data. Systems will either have to detect the privacy settings automatically, or the data will have its privacy settings permanently associated to it by the user.	Citizen Privacy will focus on providing a usable interface for end users, such as a smartphone application or a browser extension, that will allow them to specify privacy policies in a guided, thus simple and clear way. Moreover, a system for the verification of the correct behaviour of service providers will be provided, resulting in a complete privacy control mechanism for users, that will gain full control on his/her data usage. User's data will be classified according to standard privacy levels, that can be further personalised based on the needs of the individual users. This will provide a basic privacy setting for the users, in order to minimise the need for user intervention. Citizen Privacy will develop novel techniques in order to perform this classification according to user specific features, that will be in a first approximation, automatically inferred by the Trusted Platform.
Activities can include the investigation of measures to safeguard privacy in the context of mass data handling, for example where services exploiting big data, cloud services, data sharing by interconnected devices in the internet of things, and data handling in the highly sensitive context of criminal investigations.	

1.3 Concept and approach

1.3.1 Overall concept

no more than two pages

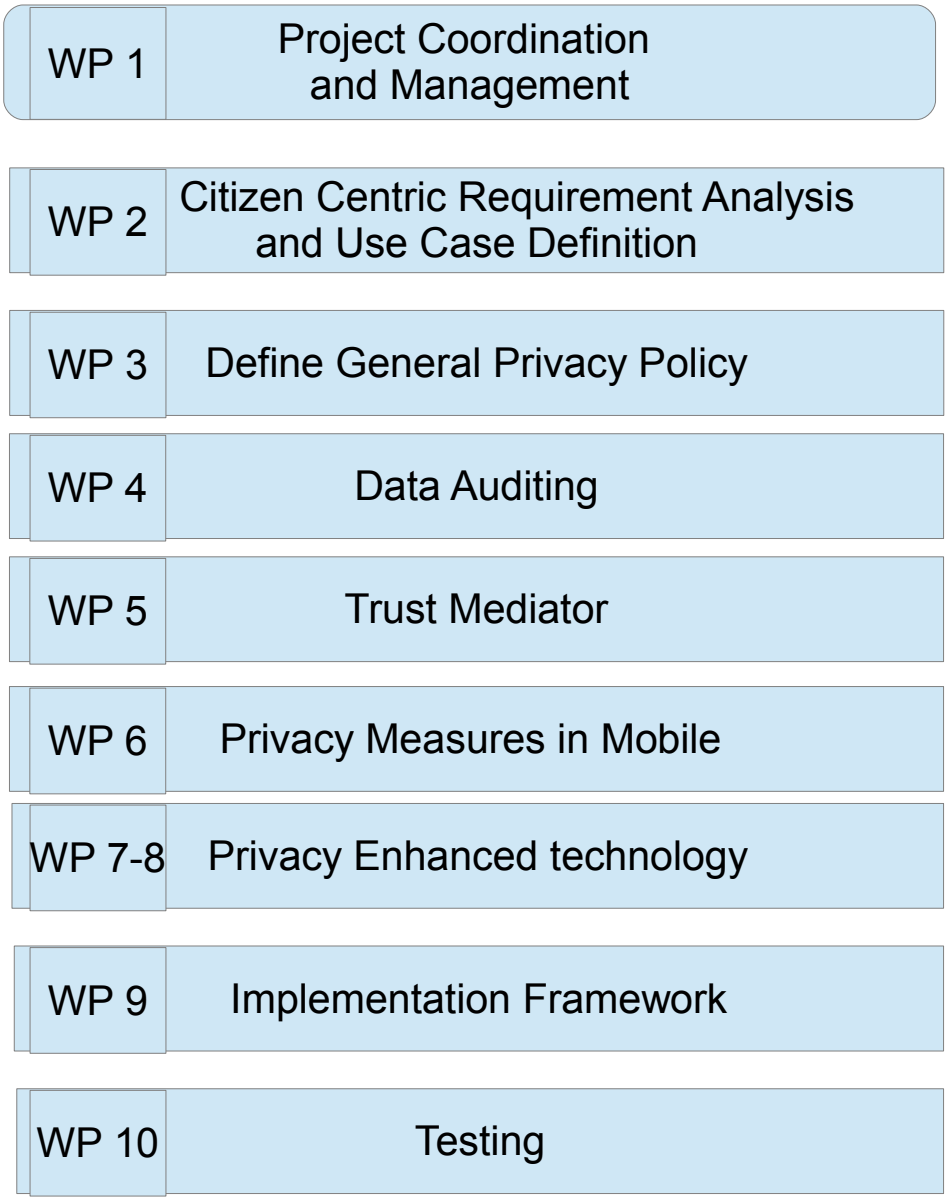

Figure 4: Work package Structure.

1.3.2 Main project results and technology readiness levels

no more than two pages

Include a half-a page figure called “Overview of the Citizen Privacy data sources, modules, apps and their interactions”

1.3.3 Linked research & innovation activities

no more than one page discuss five to eight existing works

Listed below are national and international research projects where there are already concrete opportunities for synergy, or adoption of project results, because of existing contacts from the consortium. More projects will be identified as part of WP X activities.

1.3.4 Methodology

no more than three pages including three figures

Technology enablers
Innovative models
Value networks
etc...
Figure 1 Project methodology (size 25% of the page)
Figure 2 Iterative user-driven design process (size 33% of the page)
Figure 3 Figure for various trial activities against time (size 33% of the page)

1.3.5 Privacy analysis across various division

not more than one page

e.g., include privacy attitude survey

e.g., what are the privacy attributes are sensitive to the women compared to male

1.4 Ambition

no more than a page

Our ambition is to design, build and demonstrate novel user-centric solutions that will.....

Figure 1 How different technology streams work together

1.4.1 Competitive landscape and patent review

no more than one page

The consortium has conducted an initial competitive analysis in order to identify existing..

add two small figures

Figure 1 Histograms of patents files for different user centric privacy models

Figure 2 Some collection of figures represent popular patents

1.4.2 Enabling Technologies

State-of-the-Art

no more than two pages

Topic 1: —
Topic 2: —
Topic 3: —
Topic 4: —

Project innovation
no more than two pages
Topic 1: —
Topic 2: —
Topic 3: —
Topic 4: —

1.4.3 Model Innovation

State-of-the-Art

no more than one pages

Topic 1: —

Topic 2: —

Topic 3: —

Topic 4: —

Project innovation
no more than three pages
Topic 1: —
Topic 2: —
Topic 3: —
Topic 4: —

1.4.4 Value Networks

State-of-the-Art

no more than one pages

Topic 1: —

Topic 2: —

Topic 3: —

Topic 4: —

Project innovation
no more than three pages
Topic 1: —
Topic 2: —
Topic 3: —
Topic 4: —

2 Impact

2.1 Expected impacts

2.1.1 Project impact and key performance indicators

no more than two pages

The Citizen Privacy project will provide value to all stakeholders of the value network: citizens, of course, but also service providers and network providers, infrastructure provider, research community, industry and the society at large (Table X).

The project societal impact is supported by the entire consortium, and specifically the local government actors (X, Y, Z) and the Collaborating Centres (X, Y) involved in the project.

The project industrial impact is supported by industrial partners (X,Y,Z) that will allocate substantial resources to market dissemination (WP X) and exploitation (WP X) activities.

The project scientific impact is supported by the academic and research partners (X, Y, Z) and rests on a rich set of scientific dissemination activities (please refer to section X).

Stakeholder	Call Challenges	Project Impact
Citizens	Citizens to-day share lot of information online. However they don't have any control over their data, where their data is stored and how or who uses their data. Depending on the country where the data is stored the data protection policies may vary and this will effect the confidentiality of the users data. When the service provider uses the data the end user is not benefited.	Aim of the project is to provide a trusted platform which satisfies the end-users privacy requirements.
Service provider	Users provide false information due to their concern of disclosing the sensitive data. The service provider will lose revenue because of false data provided by the end-user. Also it will have an adverse affect on the service providers reputation because of processing wrong data.	The project will enforce the service provider to use trusted platform. Hence, the end-user confidentiality will be improved as a result they are more likely to provide correct information.
Network Provider	All parties rely on data transfer and the netowrk provider plays an significant role in data communication. Providing secure data transfer will boost confidence of all the parties involved.	The project uses end-to-end anonymity protocols to ensure the data is not eavesdropped during the communication.
Infrastructure provider	Provides platform resources for processing, storing end user data.	Use TPM and encryption methods. TPM will enforce the end-user data privacy and encryption will make sure the data will be stored in a secure manner.
CZ		

The Citizen Privacy consortium has defined key performance indicators (KPIs) related to impact, that are clear, measurable, realistic and achievable (Table XX).

Table 4: Project impact indicators measured after project completion

Stakeholder	Project Impact KPI	End of project	End +5yr	End +1yr
Citizens				
Citizens				
Citizens				
Citizens				

2.1.2 Barriers / obstacles and activities required to achieve the expected impacts

no more than two pages

Include figure histogram (if possible) for the barriers

Table 5: Barriers/obstacles to impact and activities required to overcome them

Expected impact	**Barriers / obstacles**	**Activities required to overcome the barriers / obstacles and achieve the expect impact**	**WP**
Empower the citizens to manage their own privacy			
Empower the citizens to manage their own privacy			
Empower the citizens to manage their own privacy			
Empower the citizens to manage their own privacy			

2.1.3 Contribution to European innovation capacity and integration of new knowledge

no more than a page

The challenge-based third pillar of Horizon 2020 emphasises the need to take the societal problems themselves as a starting point for corporate and university research and innovation work.

The technical work of the project involves a wide range of challenging task and the interdisciplinary approach of Citizen Privacy (behavioural & social science, open data/big data, data security/privacy, user-centred design, statistical modelling/analysis, apps, policy-makers, service providers, access to end-users) requires a unique combination of skills that can only be provided by the best scientists of the USA and various European countries (UK, Norway, Denmark, Sweden, Germany, Italy, Israel)

Table 6: List of relevant standards

Standard	Privacy
ISO XXXX	
ISO XXXX	
ISO XXXX	
ISO XXXX	

2.1.4 Contribution to standards

no more than a page

The consortium has allocated sub-contracting budget to European Committee for Standardisation (CEN) to develop a CEN Workshop Agreement (CWA) focusing on the novel topic of self quantification.....

2.1.5 privacy Certification

no more than a page

2.1.6 Contributions to EC Policies and European Technology Platforms

The European Commission's Directorate General for Communications Networks.....

2.2 Measures to maximise impact

2.2.1 Joint Exploitation Plan

no more than two pages

The consortium has designed a specific methodology that will be the cornerstone of the project exploitation strategy. The method (Figure 13) is particularly well suited for Horizon 2020, as it has a major focus on market impact and support the iterative user-driven design process used throughout the project

Include a Figure called “Overview of the exploitation methodology”

Table 7: Exploitation strategy by partner in relation to the project result type

Exploitation Strategy	**Models**	**Modules**	**Apps**	**System Specs**	**System Prototype**	**Services**
Intel						
Intel						
Intel						
Intel						

All partners have also carefully considered the relevance of project results to business and other activities on completion of the project. Information on this is provided together with the description of each partner in Section XX. The output of the exploitation methodology will be a full business plan supporting the market replication of project results for each industrial partner. A preliminary business plan has been drafted based on the current understanding of the consortium and will be updated over the course of the project based on the research & innovation activities.

2.2.2 Joint Dissemination Plan

In order for Citizen Privacy to have a far-reaching impact, the dissemination strategy will encompass all stakeholders of value network (Table XX).

Disseminating project results is very important for raising awareness not only about what a project does but also about what approach it follows and why it follows it. Citizen Privacy will be using a variety of dissemination means and channels both at project and at partner level, matching the interests, the practices and the roles of the partners in the consortium (e.g. academic partners are naturally more interested in publications whereas industrial partners are more interested in business oriented and influencing dissemination). The following list summarizes the planned dissemination activities, which may be further refined and enhanced very early in the project according to the project's dissemination plan to reflect the up-to date standings of the partners involved in the consortium.

- **Project Website:** A project website will be setup and regularly updated to provide up-to-date news about the project progress, events and significant achievements. In addition it will be providing links to project material (e.g. data sets and developed software modules) that may be hosted in external repositories.
- **Public deliverables:** in order to publicly spread the results of the project, there will be provided as much public deliverables as possible.
- **Conference and journal publications:** high quality publication venues will be targeted by the project; by disseminating the project results to highly competent researchers apart from creating awareness and influencing the broader research community, useful technical feedback can be received to help steer the project's technical approach in the correct path. Envisioned targets are the following: (**International Conferences**) ACM Sensys, ACM Mobisys, USENIX Security, ACM WiSec, IEEE CNS, ACM CCS (**International Journals**) IEEE Transaction on Mobile Computing, ACM Transactions on Information and System Security, IEEE Transactions on Information Forensics and Security, IEEE Transactions on Dependable and Secure Computing.
- **Demo events and exhibitions:** the project will participate in exhibition and demo events in order to demonstrate how innovative ideas can be turned into prototypes and attract the practical interest of the industry and the wider community (e.g., FIA Future Internet Assembly, IoT Week, IoT Forum, ID-World Congress, Annual European Packaging Summit)
- **Cluster meetings:** the project will actively participate and contribute to cluster meetings to disseminate the project's results to other projects and technical-aware audience. Relevant activity chains have been identified in Table 6.
- **Presentation of tutorials in workshops:** the project will present its ideas itself in form of tutorials in workshops and conferences (e.g., IEEE ISSNIP); it will be also investigating the opportunities of co-organizing workshops together with other linked projects (e.g., Web of Things Workshop).
- **Presentations in summer schools:** the project will be participating and disseminating key material in summer schools targeting a variety of audiences with different levels of familiarity and expertise in the area and raise awareness in this broad audience (Senzations Summer School).
- **White papers:** documents that exhibit high scientific and industrial interest will be provided to the interested public.

The policy of the project towards providing and ensuring open access to the datasets and software generated during the course of the project, will be defined, implemented and updated whenever needed as part of the project's dissemination activities. This will be documented in the project's Data Management Plan (DMP) and on iterations of it when needed and one of its key objectives will be to ensure availability of datasets and software well beyond the lifetime of the project.

Table 8: Targeted audience of the Citizen Privacy project

Category Individuals	Target Citizens	Why them?	What's in it for them?

Table 9: IPR strategy related to result type

Initial agreement on IP and use rights Privacy Models	Contributing partners	Consortium partners
Statistical Data		
Software		
Apps		

2.2.3 Knowledge Management and IPR

IPR Management during the project

For the success of the project it is essential that all project partners agree on explicit rules concerning IP ownership, access rights to any Background and Results for the execution of the project and the protection of intellectual property rights (IPRs) and confidential information before the project starts. Therefore, such issues will be addressed in detail within the Consortium Agreement between all project partners. The main purpose of the Consortium Agreement is to establish a legal framework for the project in order to provide clear regulations for issues within the consortium related to the work, IP-Ownership, Access Rights to Background and Results for the duration of the project and any other matters of the consortium's interest. The Steering Committee will maintain an IPR Directory throughout the lifetime of the project. This document will list all items of knowledge relating to the work of the project (both background know-how and results developed in the project), and make explicit for each item its owner, nature, status and dissemination and protection measures. The directory will be regularly updated, and distributed to all partners. It will form a key tool to enable knowledge management.

An initial version of the IPR directory will be created at the start of the project. However, at the stage of producing the proposal, the consortium has already considered what kind of strategy should be followed concerning IPR issues for the main results of the project, and reached preliminary agreement on this. The basic principle on which we are agreed is that research and development results must be available to a large audience to facilitate wide adoption of project results, while in the meantime having options in place for rewarding those that invested. The consortium's preliminary agreement is described in Table XX.

Access Rights to Background and Results: In order to ensure a smooth execution of the project, the project partners agree to grant each other royalty-free Access Rights to their Background and Results for the execution of the project. The Consortium Agreement will define further details concerning the Access Rights after the duration of the project to Background and Results.

IP Ownership: Results shall be owned by the project partner carrying out the work leading to such Results. If any Results is created jointly by at least two project partners and it is not possible to distinguish between the contribution of each of the project partners, such work will be jointly owned by the contributing project partners. The same shall apply if, in the course of carrying out work on the project, an invention is made having two or more contributing parties contributing to it, and it is not possible to separate the individual contributions. Such joint inventions and all related patent applications and patents shall be jointly owned by the contributing parties. Details concerning jointly owned Results, joint inventions and joint patent applications will be addressed in the Consortium Agreement.

Open Source and Standards: A central aim of this consortium is to provide benefit to the European community. Some of the project partners may be either using Open Source code in their deliverables or contributing their deliverables to the Open Source communities. Alternatively, some of the partners may be contributing to Standards, be they open standards or other. Details concerning open source code use and standard contributions will be addressed in the Consortium Agreement.

Consortium Agreement: The purpose of the Consortium Agreement is to establish a legal framework for the project in order to provide clear regulations for issues within the consortium related to IP Ownership, Confidential Information, Open Source issues, Standard contributions, and Access Rights to Background and Results for the duration of the project and any other matters of the consortium's interest.

2.2.4 Open Access Strategy

no more than one page

Table 10: Individual dissemination and exploitation activity examples

Partner City	Activities during project phase	Activities after project completion
Padova		
Milano		
Darmstat		

2.2.5 Individual Dissemination & Exploitation Activities

To complement the join dissemination plan (Section 2.2.2) and the join exploitation plan (Section 2.2.1), Table XXX provides a non-exhaustive list of the individual activities planned by each partner.

The consortium has also developed a preliminary business-plan which will be updated as part of the exploitation plan iterations.

PRELIMINARY BUSINESS-PLAN FOR CITIZEN PULSE no more than two pages
Product Differentiation
Market Perception
Product Positioning
Market Segmentation
Distribution Channel
etc....

2.3 List of communication and collaboration activities

The objectives of this phase of the marketing plan are to develop awareness around the project in order to identify possible partners and end-users, that will be able to use the results of the project, either in pilots (during the project) or commercially (after project completion)

Academic dissemination: The dissemination of the project results to the scientific and academic audience will be done by publications in technical journals. The academic/research project partners .....

Project Marketing Collaterals: The industrial partners ....

Conferences & Industry Tradeshows: The project will be featured at different conferences and tradeshows. ....

Stakeholders: The partners of the project belong to several industry associations.....

Specific activities targeting SMEs: A further useful way forward to overcome these barriers is to encourage interest groups for the SMEs who can share knowledge/ know-how and give information on support required.....

Web / **Social Media Marketing:** A project web site hosted at www.CitizenPrivacy.eu .....

3 Implementation

3.1 Work plan – Work packages, deliverables and milestones

3.1.1 Overall work plan structure

no more than a page

The work plan will be implemented by a multidisciplinary, gender-balanced team of scientists, industry experts and entrepreneurs. The project starts with a specification phase focusing .....

Include a Figure Project Overview Chart (half a page)

3.1.2 Detailed work description

Gantt chart

Work package number	WP1		**Specific Objectives**				
Work package title							
Participant number							
Short name of participant							
Person/months per participant							

Objectives

Description of work (where appropriate, broken down into tasks), lead partner and role of participants

Deliverables (brief description and month of delivery)

Work package number			**Specific Objectives**				
Work package title							
Participant number							
Short name of participant							
Person/months per participant							

Objectives

Description of work (where appropriate, broken down into tasks), lead partner and role of participants

Deliverables (brief description and month of delivery)

Work package number			**Specific Objectives**				
Work package title							
Participant number							
Short name of participant							
Person/months per participant							

Objectives

Description of work (where appropriate, broken down into tasks), lead partner and role of participants

Deliverables (brief description and month of delivery)

Table 15: List of project deliverables

No D	Name	WP No	Lead	Type	Dissem. Level	Delivery Date
D						
D						
D						

Work package number			**Specific Objectives**			
Work package title						
Participant number						
Short name of participant						
Person/months per participant						

Objectives

Description of work (where appropriate, broken down into tasks), lead partner and role of participants

Deliverables (brief description and month of delivery)

3.1.3 List of deliverables

Table XX lists all deliverables in chronological order. Table 18 lists separately (as requested) formal reports.

The following numbering scheme is used:

The following numbering scheme is used: h Dw.t: Indicates that this is a deliverable from work package w, task t. Ex: D4.1 is from work package 4, task 1. h Dw.t.x : Indicates that work package w task t produces several iterative deliverables the final s provides a sequence number. Ex: D2.1.x will include several iterative releases (D2.1.1, D2.1.2 etc.) from work package 2, task 1 and only the final iteration is listed in the table and will constitute a formal deliverable (except for exploitation plan updates for which each iteration will be a formal deliverable) The deliverables list is sorted according to delivery date (as required).

Table 16: List of project milestones

Milestone No.	Milestone Name	WP	Leader	Expected Month	Means of Verification

3.2 Management structure and procedures

3.2.1 Organisational structure, milestones and decision-making

The management structure is drawn from best practices in EU projects. It utilises the principles of product-based planning, delegation of responsibility and exception-based reporting and is designed to ensure coherent scientific, administrative and financial co-ordination, while providing the participants with the support and tools required for the achievement of the project objectives.

All members of the Consortium have agreed to sign a Consortium Agreement which will codify the governance of the project as described below and to which all members will be bound.

Include Figure called “Project organisational structure”

Table 17: Decision-making mechanisms

Level Privacy Models	Decision Mechanism	Escalate if:
Statistical Data		
Software		
Apps		

Table 18: Project governance bodies

Level Privacy Models	Composition	Responsibilities
Statistical Data		
Software		
Apps		

Decision-making This section describes the most important mechanisms for reaching decisions (Table XXX), in a Consortium with multiple partners, each with their own goals. The general principle will be to try to achieve decisions by informal means and consensus, using formal procedures such as voting only when essential. Nevertheless: all decisions which can have an impact on project progress (whether reached formally or not) will be documented, for visibility within the Consortium. Precise details of the remit of the various management bodies, and of voting procedures etc. are carefully defined in the Consortium Agreement.

Conflict resolution The primary mechanism for decision-making throughout all groups within the project will be by consensus; however, where consensus cannot be reached, it is essential that processes should be available to escalate disagreements....

Project re-planning and change management

In an ambitious and dynamic project of this kind, changes to customer requirements are expected and will generate changes to the project plans. Handling changes in project plans will therefore be regarded as a normal part of project management, to be carried out without undue formalities.....

Innovation management

Innovation management is a process which requires an understanding of both market and the technical problems of the project, with a goal of successfully implementing appropriate creative ideas.....

Quality assurance

The project will employ the following mechanisms for quality assurance in the project:.....

3.2.2 Management bodies and management skills within the project

The Advisory Board will meet at least once a year (once draft progress reports have been produced), usually during a meeting of the Executive Board.....

name1
name2

3.2.3 Risk Management

no more than two pages

add Figure called “Risk Management process”

This project implementation plan, produced at the start of the project, is subject to revision in the course of the project, in accordance with the procedures for project re-planning outlined in this section.

One of the main reasons that project re-planning may be necessary is as a result of regular risk assessment in the project (Figure 17). The initial list of risks here presented in Table 23 is a start to this process; more detailed assessment of risks will be carried out regularly, based on practical experiences in running the project.

Table 19: Partner list

Category Industry/SME	Name City	Profile	Main Role

3.3 Consortium as a whole

The Citizen Privacy consortium was formed to put together a group of XXX organisations that complement each other in terms of background knowledge, technical competence, capability of new knowledge creation, business and market experience, and expertise in end-user domains where the project technologies and innovations can be readily exploited. The consortium consists of academic/research organisations, technology suppliers and end-users (Table XXX). The partners have been selected that they can contribute most effectively to different work packages. The most competent partner in the core area of each work package has been chosen as the WP Leader, taking the geographical distribution of the partners into account.

3.4 Resources to be committed

The allocation of person-month effort amongst the partners is summarised in Table XXX, according to their responsibilities and the resources estimated for achieving their assigned tasks. The overall effort of the project is 628 person months over the XX years. The details of cost allocation per partner are summarised in Table XXX.