Project Acronym:	**VICINITY**
Project Full Title:	**Open virtual neighbourhood network to connect intelligent buildings and smart objects**
Grant Agreement:	**688467**
Project Duration:	**48 months (01/01/2016 - 31/12/2019)**

Deliverable D10.2

Risk Assessment, Ethical monitoring and Contingency Plans

Work Package:	**WP10 – Project Management**
Task(s):	**T10.2 – Quality Assurance, Risk and Ethics Management**

Lead Beneficiary:	**CAL**
Due Date:	**30 Sept 2016 (M9)**
Submission Date:	**30 Sept 2016 (M9)**
Deliverable Status:	**Draft**
Deliverable Type[1]:	**R**
Dissemination Level[2]:	**PU**
File Name:	VICINITY_D10 2_ risk_mgmt_ethical_contingency_v1 0-final.docx

This project has received funding from the European Union's Horizon 2020 Research and innovation programme under Grant Agreement n°688467

VICINITY Consortium

No	Beneficiary		Country
1.	TU Kaiserslautern (Coordinator)	UNIKL	Germany
2.	ATOS SPAIN SA	ATOS	Spain
3.	Centre for Research and Technology Hellas	CERTH	Greece
4.	Aalborg University	AAU	Denmark
5.	GORENJE GOSPODINJSKI APARATI D.D.	GRN	Slovenia
6.	Hellenic Telecommunications Organization S.A.	OTE	Greece
7.	bAvenir s.r.o.	BVR	Slovakia
8.	Climate Associates Ltd	CAL	United Kingdom
9.	InterSoft A.S.	IS	Slovakia
10.	Universidad Politécnica de Madrid	UPM	Spain
11.	Gnomon Informatics S.A.	GNOMON	Greece
12.	Tiny Mesh AS	TINYM	Norway
13.	HAFENSTROM AS	ITS	Norway
14.	Enercoutim – Associação Empresarial de Energia Solar de Alcoutim	ENERC	Portugal
15.	Municipality of Pylaia-Hortiatis	MPH	Greece

[1] ***Deliverable Type:***
R: Document, report (excluding the periodic and final reports)
DEM: Demonstrator, pilot, prototype, plan designs
DEC: Websites, patents filing, press & media actions, videos, etc.
OTHER: Software, technical diagram, etc.

[2] ***Dissemination level:***
PU: Public, fully open, e.g. web
CO: Confidential, restricted under conditions set out in Model Grant Agreement
CI: Classified, information as referred to in Commission Decision 2001/844/EC.

Authors List

Leading Author (Editor)			
Surname	**First Name**	**Beneficiary**	**Contact email**
Wall	Nigel	CAL	nw@nigel-wall.co.uk

Co-authors (in alphabetic order)				
No	**Surname**	**First Name**	**Beneficiary**	**Contact email**
1.	Grimm	Christoph	UNIKL	grimm@cs.uni-kl.de
2.	Samovich	Natalie	ENERC	n.samovich@enrcoutim.eu

Reviewers List

List of Reviewers (in alphabetic order)				
No	**Surname**	**First Name**	**Beneficiary**	**Contact email**
1.	Ananika,	Alexandra	MPH	a.ananika@pilea-hortiatis.gr
2.	Dickerson	Keith	CAL	keith.dickerson@mac.com
3.	Nygaard	Erik	TYNM	en@serinustechnology.com
4.	Sveen	Flemming	HITS	flsveen@online.no
5.	Tryferidis	Thanasis	CERTH	thanasic@iti.gr

Revision Control

Version	Date	Status	Modifications made by
0.1	Feb 2016 (M2)	Initial Draft	Wall (CAL)
0.2	July 2016 (M7)	Draft	Wall (CAL)
0.3	August (M8)	Extended CG	Grimm (UNIKL)
0.6	September, 15	Ethics Board Details	Samovich (ENERC)
0.7	September, 19	Add more detail	Wall (CAL)
0.9	September, 22	FMEA added, Layout finalized	Grimm (UNIKL)
0.10	September 23	Inconsistencies corrected + English edits	Wall (CAL)
0.11	September 23	Draft for QAR	Dickerson (CAL)
0.12	September 28	Final Draft reviewed	Dickerson (CAL)
1.0	September, 30	Submission to the EC	Grimm (UNIKLK)

Executive Summary

The present document is a deliverable of the VICINITY [1] project, funded by the European Commission's Directorate-General for Research and Innovation (DG RTD), under its Horizon 2020 Research and Innovation Programme (H2020) [2].

The deliverable covers three important topics:

- It establishes the process to be used to identify, record, manage and monitor risk and the need for contingency planning when an identified risk cannot be completely avoided or mitigated.
    - The Risk Register will be maintained as a specific project management document, stored on OwnCloud. The template for the Risk Register is included as Annex A. The template included here has not been populated, but the actual Risk Register has been created using the initial risks identified in the Description of Work. Always consult the latest Risk Register on OwnCloud at: https://cpsgw.cs.uni-kl.de/cpscloud/index.php/apps/files/?dir=%2FVICINITY4Consortium%2FRisk%20Register
- It describes how Failure Mode and Effect Analysis (FMEA) will be applied to the Risk Register to put in place appropriate contingency plans
- It defines the way that the project's Ethics Advisory Board (EAB) will operate, and sets out a policy for ensuring the privacy of any person who becomes involved with the VICINITY trials.
    - The template form has been created for obtaining the informed consent of any data subject / participant who will be involved with VICINITY trials. This is included as Annex B of this document.
    - The Data Management Plan is presented: this will be overseen by the EAB.

The Project Quality Board will review this document and suggest revisions if these are found to be needed during the life of the project.

Table of Contents

List of Tables

List of Figures

List of Definitions & Abbreviations

Abbreviation	Definition
DoA	Description of Actions / Grant Agreement Annex 1
DPO	Data Protection Officer
EAB	Ethics Advisory Board
EC	European Commission
EFMEA	Extended Failure Mode and Effect Analysis
EGE	European group on ethics
EU	European Union
FMEA	Failure Mode and Effect Analysis
FMCA	Failure Mode and Effect Critical Analysis
GA	General Assembly Meeting, ½ yearly of VICINITY partners
GDPR	General Data Privacy Regulation
HAZOP	Hazard and Operability Studies
GR	Greece
NO	Norway
P&ID	Piping and Instrumentation Diagram
PC	Project Coordinator
PT	Portugal
PO	Project Office
QAR	Quality Assurance Review
RADM	Risk Assessment Decision Matrix Analysis
RPN	Risk Priority Number

1. Introduction

This document has been produced within Task 10.2, which has the following brief. Those aspects that are covered by those document are highlighted by **emboldened text**

T10.2 Quality Assurance, Risk and Ethics Management (M1, M48)
Leader: ***CAL (3)*** *Contributors: UNIKL(4),CERTH(3),ITS(1),ENERC(2),MPH(2)*

This task will set up a Project Quality Board consisting of the Project Coordinator, the Technical Manager, the Quality Manager, Users Representative and a person in charge of Standards. A Quality Assessment Plan will be produced at the beginning of the project (Month 6) that describes in detail the quality requirements of the project and the respective guidelines in order to achieve this quality level. In addition**, this task will deliver a detailed contingency plan for the technical and other objectives of the project that will be continuously updated during the project lifetime. A detailed risk assessment will be performed for all modules that comprise the VICINITY system, along with the proposed mitigation actions following well established methodologies (e.g. Failure Mode and Effects Analysis). Finally, VICINITY will establish an Ethical Advisory Board - EAB to provide ongoing support to the consortium concerning ethical and legal issues. The main tasks and responsibilities of the EAB will be to ensure that the project is proceeding in a responsible and ethically acceptable manner, while an ethics helpdesk will be established at M12 to address all ethical issues for use case activities. Furthermore, this task will identify and include all relevant national and international European legislation and directives related to the countries where the data collection will take place.**

There are two deliverables from this Task:

D10.1: Project Management, Quality Assessment Plan (M6) that describes the general management processes, and

D10.2: Risk Assessment, Ethical monitoring and Contingency Plans (M9) that gives details on Risk/Contingency management and Ethical monitoring.

1.1 Relevant sections of the DoA and D10.1

The DoA gives in Section 3.2.1.15 (Emergency Cases and Risk Management), Section 3.2.3 (Critical risks) and in 3.2.1.7 (Ethics Advisory Board) an indicative direction. Based on these Sections of the DoA, D10.1 (Project Management and Quality Assessment Plan), Section 4.5, gives a more concrete description of risk management that we describe in this deliverable in more detail.

1.1.1 Risk Management and Risk Register

Risk management as part of the overall management process was introduced in D10.1, where it was described as follows (D10.1, Section 4.5):

For risk management, a Risk Register has been created, based on the initial risks from the proposal and is continuously updated as soon as risks become visible. Then, immediately we will investigate mitigation strategies. The updates are communicated in the half-yearly periodic reporting deliverables.

As soon as the PC detects problems, which can endanger the objectives of the project, such as serious delays of deliverables, he will call for an extraordinary Plenary Board meeting. In this meeting, the situation will be analysed by consensus and a decision will be proposed in order to solve the problem. Any conflicts that cannot be resolved through the principles above will be handled according to the dispute

resolution provision set forth in the CA. The Risk Management and Contingency Plan, as well as the Quality Control Plan discussed above are handled both at the WP level, as well as centrally within WP10.

Actions and processes taken for assessment, monitoring of risks, and for contingency management are described in Section 2 of this deliverable, where the structure of the Risk Register is described in detail. The format of the Risk Register is presented in Annex 1.

1.1.2 Ethical Monitoring

The DoA (3.2.1.7) describes the Ethics Advisory Board as:

"An Ethics Advisory Board will be established for the whole project lifetime to address any legal and ethical issues for the technologies developed by the consortium and assist in the preparations and execution of the field and lab trials. The Ethics Advisory Board will address privacy issues related to data collection and handling, providing its valuable input and responses to consortium partners involved in the development and realisation of the trials, as well as actual end-user participants."

This group includes one representative form each country where a VICINITY pilot trial will be operated: the national pilot representative shall also act as the Pilot sites' Data Protection Officer (DPO) - a position that is required by the new General Data Privacy Regulation (GDPR) [3]. The DPOs will facilitate liaison with each pilot to ensure that each trial meets the legal and best-practice requirements that VICINTY will adopt. The DPOs will also manage the liaison with national authorities to ensure that any additional National Requirements are accommodated.

1.2 Failure Mode & Effect Analysis (FMEA)

A five stage Risk Management Plan has been adopted for the needs of VICINITY including: *Risk Identification*, *Risk Quantification*, *Risk Response Development*, *Risk Monitoring and Control*, and *Risk Documentation*:

- *Risk Identification* examines the risks that can affect the project documenting the characteristics of each one.
- *Risk Quantification* involves the evaluation of risks by determining the interactions, relationships and implications to the project, identifying probabilities of occurrence and assessing the possible effects.
- *Risk Response Development* involves the management of risks by determining response strategies plan, project reserves and mitigation strategies.
- *Risk Monitoring and Control* involves controlling risks, making decisions on how to handle each situation, and take correct actions. The main products are a risk registry, corrective actions and updates to the risk management plan.
- *Risk Documentation* contains the project database development for collecting historical information on the risks encountered.

For the first three stages a formal Risk Analysis and Assessment method is needed. Currently, over 100 Risk Analysis techniques are available in the literature. The most common traits of them are the identification of initiating events (causes), consequences, safeguards, and recommendations. The alternative techniques have been reviewed and an analysis is included in section 2.1 For VICINITY we shall use "Expanded Failure Modes and Effects Analysis" (EFMEA).

2 VICINITY Risk & Contingency Management

2.1 Choice of the FMEA technique to be used

There are several well established FMEA techniques that differ in the way they identify causes or consequences. The five most popular techniques are "Hazard and Operability studies" (HAZOP), "Failure Modes and Effects Analysis" (FMEA) or "Failure Mode, Effects and Critically Analysis" (FMECA), "Expanded Failure Modes and Effects Analysis" (EFMEA), "What if" and "Risk Assessment Decision Matrix Analysis" (RADM). These methods are briefly described below:

Hazard and Operability Studies (HAZOP)

HAZOP is a regulated methodological technique for analysing hazards and operational concerns of a system, often used in chemical industries. According to *HAZOP*, normal and standard operations are safe and hazards occur only when there is a deviation from the normal operation.

Failure Modes and Effects Analysis (FMEA / FMECA)

FMEA evaluates the effects of potential failure modes of subsystems, assemblies, components and functions using design and failure knowledge as inputs. Its concept is based on the following questions: What can fail? How does it fail? How frequently will it fail? What are the effects of the failure? What is the reliability/ safety consequence of the failure?

Expanded Failure Modes and Effects Analysis (EFMEA)

EFMEA has been designed in order to overcome some of the FMEA limitations. This method provides information to identify critical elements of the overall system, evaluate suitable actions and mitigation strategies, with the overarching goal of contributing to the contingency plans of the project. In EFMEA risk analysis is conducted in two stages: Risk Identification and Risk Mitigation. Also, EFMEA classifies Risks into four categories:

- Technical (physical features of hardware; coding elements of software)
- Legal (based upon existing policies and laws in each nation)
- Behavioural (resulting from user's behaviour)
- Organisational (in relation to disaster mitigation plans and actor's roles).

To match the needs of VICINITY, we refine this classification in Section 3.

What-if Analysis

What-if is an inductive method similar to *HAZOP* (although much less systematic and more intuitive). It is actually a brainstorming approach in which a group of experienced people familiar with the subject process raise the question "what-if" instead of using keywords when examining the P&ID (Piping and Instrumentation Diagram) of the system and voice concerns about possible undesired events.

Risk Assessment Decision Matrix Analysis (RADM)

The *RADM* is a technique which uses a graphic representation of the severity or damage of an accident and its occurrence probability. It provides a quick view of risk ranking in different process hazard analysis (e.g. *HAZOP*).

Taking into account the inputs and outputs of each method, the advantages and disadvantages, as well as the evaluation in the literature among Risk Analysis Methods in reasearch environments, (adapted) **EFMEA has been selected as the best and most suitable approach to meet the needs of VICINITY**. EFMEA is a detailed, rigorous method, relatively inexpensive, which accepts a high degree of complexity and is commonly used in a variety of industries for Risk Management, where simple quantification of risk is insufficient, and where identification of root causes of risks and means of mitigation are paramount.

In EFMEA results can be correlated directly with actual risks and the effect of various methods of mitigation/detection on risk can be easily modelled. Moreover, it provides a well-documented record of improvements from the corrective actions implemented as well as useful information in developing test programs and in-line monitoring criteria. It also provides historical information, which is useful in analysing potential failures during the project lifecycle.

2.2 Identification of risks

The Risk Register is a key document for the management of the VICINITY project.

The Risk Register shall be maintained to allow the project to identify, assess and manage risk, tracking its mitigation as work proceeds. The format of the Risk Register is shown in Appendix A of this document and its operation is explained in section 2.3 below.

The Risk Register can be found at https://cpsgw.cs.uni-kl.de/cpscloud/index.php/apps/files/?dir=%2FVICINITY4Consortium%2FRisk%20Register which may need the password VICINITY to allow access.

The process for identifying and reporting risks is as follows:

1. When a member of the consortium becomes aware of a risk that may harm the work of the project, they should **immediately** discuss this with
    a. the WP leader(s) and then
    b. the PC and management board via the Project Office (PO) (Carna Radojicic)

    Then, the Risk Register will be updated by the PO to record this new risk.

2. At the half-yearly General Assembly meetings, the risks and mitigation plans are discussed with all partners. Additional risk may be identified during these discussions, and should be captured.

3. The WP leaders and the management board will discuss, together with the persons involved, a contingency plan that mitigates the risk. The level of detail of the contingency plan depends on the likelihood and significance of the risk.
    a. If a risk is unlikely, the management board will just add some possible options; the more likely a risk becomes, the more detailed the contingency plans will be made.
    b. In case a risk seems to be very likely, a detailed contingency plan will be established as required.

The template for the risk register is in Annex A. This may be updated continuously. The most recent version is always in the OwnCloud repository in the folder /Reporting/Risks.

The updates are communicated in the half-yearly periodic reporting deliverables.

2.3 The Risk Register format

The Risk Register contains a number of columns under which each risk is analysed individually. The Risk Register has been created in Excel, which allows the order and grouping of the risks according to the information in any of the columns. These columns are:

- **Risk identification number.** This is a simple serial number. The order of the risks is simply the order in which the risk was added to the list.
- **The type of risk**. The following types have been identified:
  - Gen: General risk
  - Tech: Technical risk
  - Case: Use Cases Risks, tests at use cases
  - Man: Management risk
  - Expl: Exploitation (commercial) risk
  - Ethics: Ethical risks, including privacy legal concerns.
- **Work-packages** affected by the risk
- **Risk Event:** the definition of what might go wrong, and how this might be caused.
- **Risk Impact:** what would be the impact on the project if the risk event happened.
- **Origin:** this records how the risk was identified: this may be the name of an individual or a partner, or it may be an output from a project meeting. The initial items in the Risk Register are those that were included in the project proposal, where the Origin is shown as Prop.
- **Probability**, that the risk event will occur: *High = 5, Low = 1*
- **Consequence**: severity of the impact should the risk event occur: *High = 5, Low = 1*
- **Overall Risk**: *Risk = sqrt(Probability x Consequences)*
- **Mitigation Action Plan:** specific steps that will be taken to ensure that the probability and impact of occurrence will be minimised.
- **Mitigation Action Feasibility:** Describes to what extend the Mitigation action is able to reduce the impact of a risk event. *Low=5, High=1*
- **Status**: whether the proposed mitigation has been put in place, and indeed recording if a risk event does occur.
- **Risk After** – is a calculation of residual risk after the mitigation
- **Risk Difference** to record FMEA-based assessment of mitigation actions.

The Risk Register template is shown as Annex A to this document. The current version of the Risk Register can be found under the link https://cpsgw.cs.uni-kl.de/cpscloud/index.php/apps/files/?dir=%2FVICINITY4Consortium%2FRisk%20Register

2.4 Use of the Risk Register

Risks should be added to the Risk Register, by the PO, as and when members of the consortium identify and report a new risk, based on (Expanded) FMEA described in Section 3.

The Risk Register will be reviewed at each plenary project meeting in order to check:

- That each risk and its impact has been understood.
- That everyone is aware of the potential impact on their work.
- That an appropriate mitigation plan has been developed and is being acted upon.
- That everyone is aware of what they need to do to mitigate the risks.

When updated, the Risk Register should have its serial number updated within the file but should be saved using the initial name under the link: https://cpsgw.cs.uni-kl.de/cpscloud/index.php/apps/files/?dir=%2FVICINITY4Consortium%2FRisk%20Register

3 VICINITY (Expanded) Failure Mode and Effects Analysis

3.1 Methodology

This section first describes the methodology of the Expanded Failure Modes and Effects Analysis method in general. Initially, we provide a brief description of the classic FMEA.

FMEA is an analysis technique that facilitates the identification of potential problems in the design or process of a system by examining the effects of lower level failures. Recommended actions or compensation provisions are made to reduce the likelihood of the problem occurring, and mitigate the risk, if in fact, it does occur. The FMEA determines, by failure mode analysis, the effect of each failure and identifies single failure points that are critical. It may also rank failure according to the criticality of a failure effect and its probability of occurring. This course of action, if succeeded, helps to identify potential failure modes based on past experience with similar products or processes, enabling those failures to be designed out of the system with the minimum of effort and resource expenditure, thereby reducing development time and costs. Some definitions are given below:

Failure Modes are the ways, or modes, in which something might fail. Failures are any errors or defects, especially ones that affect the customer, and ca be potential or actual.

Effect Analysis refers to studying the consequences of those failures and can help to identify potential mitigation strategies.

According to the seriousness of the consequences, the frequency of occurrence and their detectability, failures are prioritized. The combination of these three factors gives the Risk Priority Number (RPN) for each failure mode identified in the system. The purpose of the FMEA is to take actions to eliminate or reduce failures, starting with the highest-priority ones. This procedure is depicted in Figure 3-1.

1.

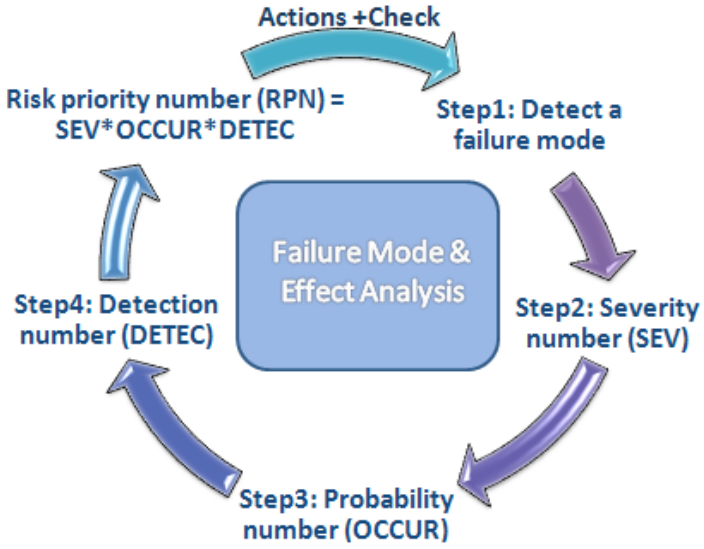

Figure 3-1: FMEA Process Cycle (source: Dieter Vandeun, commons.wikimedia.org)

FMEA is a popular and broadly accepted methodology for Risk Analysis, which has been adopted by various projects. However, it has been criticized for having a number of limitations throughout the various calculations steps, such as tediousness, missing key failures and inability to affect key process decisions if performed too late.

As it has already been mentioned, within the scope of VICINITY, (adapted) EFMEA designed to overcome some of the FMEA limitations, is being used. In the next sections a brief description of the respective methodology is presented.

3.1.1 Calculation of Severity, Probability and Risk number

Whilst many (E)FMEA are carried out by teams of experts, the VICINITY consortium consists of partners from different countries working independently. Therefore, ways of achieving consistent and quantifiable results from all partners are required. The following checklist of 10 key points based upon the question "What can go wrong?" has been developed by Bluvband and Grabov [12] to assist individuals in identifying possible Failure Modes introduced by events:

1. The intended function is not performed
2. The intended function is performed, but there are some safety problems, or a problem in meeting a regulation associated with the intended function performance
3. The intended function is performed, but at a wrong time (availability problems)
4. The intended function is performed, but in the wrong place (position in the system)
5. The intended function is performed, but in the wrong way (efficiency problems)
6. The intended function is performed, but the performance level is lower than expected
7. The intended function is performed, but its cost is higher than planned (additional maintenance, repair, power consumption etc.)
8. An unintended/unplanned and/or undesirable function is performed

9. The period of intended function performance (lifetime) is lower than planned (reliability issues)

10. Support for the intended function performance is impossible or problematic (maintenance, repair, service issues etc.)

Based on the overall approach, the following tables have been developed to assist in identifying the level of each risk and the value that should be assigned in the RPN calculation.

We define the levels of probability as follows:

Level	Probability of an event
1	The event is extremely unlikely
2	The event is unlikely to occur
3	The event might occur
4	The event is likely to occur.
5	The event is very likely or certain to occur.

The levels of consequences (severity) are as follows:

Level	Consequences of an event
0	The event will have no impact
1	The impact will have isolated impact not above task-level
2	The event will have impact on work packages.
3	The event will have impact beyond work packages.
4	The event will have impact on the overall project, but limited to single deliverables or parts.
5	The event will have serious impact on major mission and results as promised in the DoA.

For the sake of intuitive use by non-experts we normalize in the following all numbers and means to the range 0-5.

Based on this common quantification approach of (subjective) probabilities and severities of failures, we can compute quantitative risk numbers. Risk numbers (Overall Risk in Section 2.3) are computed considering the probability of its occurrence and its Consequences using the following equation; we get a normalized range between 0 and 5 as follows while maintaining intuitive semantics of the chosen levels:

$$RPN = Risk = \sqrt{Probability * Consequences}$$

Based on the quantified risk we are then able to compare risks and to find out the most dangerous ones based on a quantitative approach. Note, that in deviation to Figure 3-1 we don't estimate the likelihood of detection and that we normalize the numbers for quantification to the range of 0-5.

The next step is to attempt to prioritise the risks in order of their criticality. It is important to not adhere to pre-specified thresholds (e.g. RPN >= *X)*, as too low a threshold can lead to substantial corrective work, some of which may not be required. Selecting a top 10, or the highest 5% can also be problematic, and so all items are to be ordered in a list, from the highest RPN to the lowest RPN and then plotted as a 'scree plot' (see Figure 3-2 below). The uppermost values (i.e. those not on the lower trend line) are marked and potential mitigation strategies for these specific items are then determined.

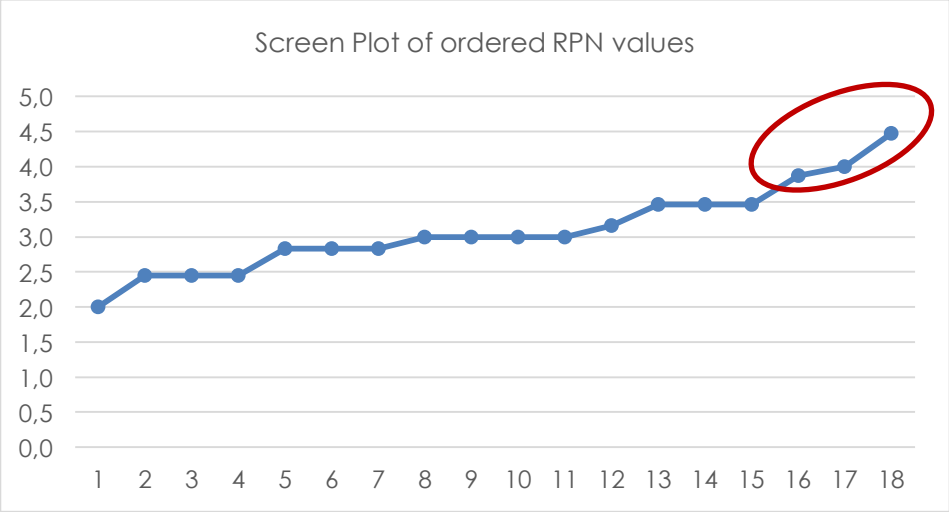

Figure 3-2: Example of analysis of risk values.

3.1.2 Mitigation action plan

Once the critical items have been identified, the next step is to identify possible corrective actions or mitigating strategies. The possible success of these actions/strategies should also be identified and, where possible, quantified. There may be several possible options for each issue, and any risk reduction is an iterative process involving dependencies between the different issues.

In terms of corrective actions, risk can be reduced in a number of generic ways:

- reducing the magnitude (severity) of the consequences of the potential risk;

- reducing the probability of the risk occurring;
- increasing failure detection speed and probability;
- protecting against the risk, mitigating strategies to compensate for a failure;

Traditional FMEA does not issue adequate guidance for selecting the optimal choice of corrective action, as actions required to lower existing RPN values may not be appropriate, achievable or feasible under project constraints (time, resource, budget etc.) Therefore, Bluvband and Grabov [11] propose a comparison evaluation of each pre- and post-correction RPN, also taking into account the 'feasibility' of each action.

The 'feasibility' of each action is ranked on a scale from 1 (Best Case) to 5 (Worst Case), using the following table:

Feasibility of Corrective Action Implementation	Ranking
Safety problem and/or non-compliance to Government regulations; Unavailable necessary resources; Unacceptable cost/time/resource consumption; Zero chance of success; 100% probability of undesirable impact	5
Remote availability of necessary resources; Near unacceptable cost/time/resource consumption; Remote chance of success; ~80% probability of undesirable impact	4
Low availability of necessary resources; High cost/time/resource consumption; Low chance of success; ~60% probability of undesirable impact	3
Moderate availability of necessary resources; Medium cost/time/resource consumption; Moderate chance of success; ~40% probability of undesirable impact	2
Full availability of necessary resources; Very low cost/time/resource consumption; High chance of success; 0-10% probability of undesirable impact	1

To quantify the remaining risks after (RPN values) after possible mitigation actions, we multiply the RPN value with the values from the above table, scaling it to the range 0-5 again to allow a ranking of risk numbers (RPN values) after mitigation actions; we use the following formula:

$$Risk\ after\ mitigation = \sqrt{Feasibility * Risk\ before\ mitigation}$$

The difference between the RPN value before and after mitigation actions is used to assess a ranking and selection of mitigation actions.

3.2 VICINITY EFMEA

In VICINITY, risk management considers that in complex projects many issues cannot be anticipated in advance, but can be detected early enough within project runtime. For that reason, we continuously (at GA meetings, for example) check with all participants for potential new risks and perform a subsequent update of the risk table and decide which mitigation actions should be started. The half-yearly status reports (D10.3+) contain these updates of risk table and mitigation actions.

The EFMEA of the initially identified risks, including the updates from the first half-yearly status report from M6 is briefly described below.

3.2.1 Risk analysis (after GA1/M06)

In the following table the Risks are listed as maintained in the Risk Register, sorted by ID.

Table 3-1: Risk analysis for Risk Register as of M06 (after GA1)

ID	Type	WP	Risk event	Impact	Proba-bility	Conseq-ense	Risk
1	Gen	WP1	Distorted image of the user group and system requirements	The project partners may design an approach that would not fit with stakeholder requirements. In which case it would be unlikely to succeed commercially.	3	3	3,0
2	Gen	WP1	Requirements are too generic or incomplete	The project partners may design an approach that would not fit with stakeholder requirements. In which case it would be unlikely to succeed commercially.	3	3	3,0
3	Gen	WP3, WP4, WP5, WP8	Privacy concerns or loss of privacy control	Within VICINITY, data sharing between smart objects of different owners will be performed. This may raise serious privacy issues. The new DGPR sets clear requirements that must be implemented from 2018. Failure to meet these obligations would require a rework of VICINITY's trial, proposed product and	2	5	3,2

				services if this regulation is not included from the outset.			
4	Tech	WP6, WP8	Timely response of the system is not appropriate leading to difficulties in use	The integration of many different and heterogeneous IoT applications brings a risk of reducing the speed of the final system making it difficult to use.	3	5	3,9
5	Tech	WP6	Integration with existing heterogeneous systems fails	Incremental introduction would not be possible wit the ability to connect with other systems.	3	4	3,5
6	Tech	WP3 WP4	Lack of IoT protocol interoperability	Current IoT networks are often vendor locked by design. This may lead to interoperability issues, since IoT component vendors might be reluctant to share interface specifications.	2	4	2,8
7	Tech	WP3 WP4	Automatic mapping of newly discovered IoT descriptors systematically unsuccessful due to unexpected semantic structures	such an approach would be locked in time and unable to adapt to evolution of technology.	2	4	2,8
8	Tech	WP8	Poor system performance leads to the failure of demonstrations	Poor quality demonstrations would undermine confidence in the VICINITY project and would waste an opportunity to demonstrate excellence.	2	3	2,4
9	Tech	WP8	Appropriate users are not available to validate the system platform.	Delays would mean that the duration and extent of trials would be limited.	3	3	3,0
10	Expl	WP9	Disputes over ownership of IPR amongst consortium partners	exploitation opportunities would be limited if partners were not able to benefit from all the innovation arising from the project	2	4	2,8
11	Expl	WP9	Breach of IPR conditions within consortium agreement	exploitation opportunities would be limited if partners were not able to benefit from all the innovation arising from the project	1	4	2,0
12	Expl	WP9	Lack of interest on the VICINITTY project by external stakeholders	The project would lose the value from guidance provided by external stakeholders	3	4	3,5

13	Man	WP10	Partner leaves Consortium	A gap might be left which meant the project could not complete its full scope.	2	3	2,4
14	Man	WP10	Key staff illness/leave during critical project phase	A gap might be left which meant the project could not complete its full scope.	2	3	2,4
15	Man	All	Poor quality of deliverables and delay in meeting the deadlines	Delays in deliverables may cause ongoing delays within the project. However, poor quality deliverables could result in wasted effort as the wrong direction would be set.	4	3	3,5
16	Case	WP7, WP8	Pilot site delayed or not available any more	We are not able to set up all planned use cases and to demonstrate and evaluate the value-added services as foreseen in WP7/8.	5	4	4,5
17	Man	All	Partner experts are not paid monthly salary nor having their travel reimbursed	Substantial delay in partner deliverables	Prop	4	4
18	Man	All	Partner is not contributing to tasks according to their budget	Substantial more work on the other partners and delay	GA1	3	3
19	Gen	WP7, WP8	Volunteers at the Greek test site may find the service is intrusive and ask to be removed from the trial	If volunteers withdraw it may not be possible to use their historic data and the trends monitoring will be incomplete leading to incomplete result	QAR	3	3.5

Risks with a high risk number (3.5+) are identified as

- **ID 16:** Delay of a pilot site (See also D10.3) with risk number = 4,5.
- **ID 4:** Timely response of the system is not appropriate.

For ID 16, we started mitigation actions as described in deliverable D10.3.

For ID 4, in the requirements phase we define an architecture that allows us to achieve a very high performance regarding response time.

3.2.2 Mitigation actions

The mitigation actions and their feasibility and impact on the overall risk (Delta Risk) are listed in the table below as calculated by the Risk Register:

Table 3-2: Mitigation Action Plan

ID	Risk event	Risk	Mitigation Action Plan	Feasi-bility	Status	Risk after	Delta Risk
1	Distorted image of the user group and system requirements	3,0	VICINITY will analyse the perspectives of the different stakeholders groups, which will be early engaged in the project and will consider all the feedback derived, ensuring a well-rounded information base for the user and environment requirements. An EAB will be established, which will help throughout the project lifecycle.	1	ongoing	1,7	**1,3**
2	Requirements are too generic or incomplete	3,0	An explicit definition of the barriers, trade-offs & sensitivity points will take place from the beginning of the project so that risk mitigation can be facilitated. The set up of the EAB will mitigate this risk, as requirements will be collaborated with end-users and negotiated with stakeholders' representatives and experts. The lessons learned and iterative processes will allow requirements to be refined.	1	reduced by D1.2	1,7	**1,3**
3	Privacy concerns or loss of privacy control	3,2	An EAB has been established to ensure that GDPR is complied with, and best practice adopted. VICINITY concept preserves user's privacy by design and no central databases with sensitive data are planned. Also, during pilot realization only modern privacy preserving systems and equipment will be used and any original records or data will be destroyed after their processing for the extraction of context-aware knowledge. Additionally, no algorithmic mechanisms will be realised for the assessment of any behaviour outside the spectrum of work related tasks.	1	ongoing	1,8	**1,4**
4	Timely response of the system is not appropriate leading to difficulties in use	3,9	The sensing and communication structure of the system will be carefully studied and designed in order to exclude any overlapping sources of data or sources of low information value.	2	ongoing	2,8	**1,1**
5	Integration with existing heterogeneous systems fails	3,5	The design and implementation of components should be strictly decoupled from all tool-specific details. Interfaces should be compatible with the existing standards.	2	ongoing	2,6	**0,8**

6	Lack of IoT protocol interoperability	2,8	VINICITY will mitigate this risk by establishing new open general specifications, so that system vendors can easily get connected with the help of open source samples for adapter implementations without the necessity to share their specifications and source codes.	1	ongoing	1,7	**1,1**
7	Automatic mapping of newly discovered IoT descriptors systematically unsuccessful due to unexpected semantic structures	2,8	Such descriptors will be inserted into a pool for investigation by developers. Then, they can be integrated manually and the discovery logic will be modified to discover similar structures since that time. This will lead to an incremental process towards the improvement of auto-discovery features.	1	ongoing	1,7	**1,1**
8	Poor system performance leads to the failure of demonstrations	2,4	Pilot environment conditions will be closely monitored, so that the causes of poor performance can be identified and used for the optimisation of the system, and the prevention of future system failures.	2	ongoing	2,2	**0,2**
9	Appropriate users are not available to validate the system platform.	3,0	User partners have already been carefully selected to ensure that they are suitable for the pilot tests. Additional users will be identified as part of the use case demonstration process and will be kept as potential backup if required.	1	ongoing	1,7	**1,3**
10	Disputes over ownership of IPR amongst consortium partners	2,8	Standard IPR and access rights clauses have been included in the Consortium Agreement, which has been signed before work starts to avoid disputes. Any dispute concerning this aspect will be solved based on what all partners have signed in the Consortium Agreement, using the methodology agreed for problem resolution.	1	consortium agreement in place	1,7	**1,1**
11	Breach of IPR conditions within consortium agreement	2,0	The IPR clauses were properly understood before signing the Consortium Agreement. The Consortium Agreement also includes liability of the partners in case they do not follow any of the agreed terms.	1	consortium agreement in place	1,4	**0,6**
12	Lack of interest on the VICINITTY project by external stakeholders	3,5	The Task partners on this part of the project will manage a continuous operation on communication channels in order to keep in touch with multiple stakeholders. Also, various dissemination activities will be carried out to raise the awareness and increase the interest into the results of the project. The dissemination and communication plan will be periodically (every year) updated to address potential issues that can be faced by the project.	1	ongoing	1,9	**1,6**

13	Partner leaves Consortium	2,4	Consortium is of sufficient strength and diversity so that partners can be replaced if required. Also, the coordinator will ensure appropriate control and management of the work in progress so that the remaining partners can complete the work, until a new partner is found (in case that is considered necessary).	1	ongoing	1,6	**0,9**
14	Key staff illness/leave during critical project phase	2,4	All partners have experienced staff that may replace and take over the work assigned to the leaving member, either temporarily or permanently.	1	ongoing	1,6	**0,9**
15	Poor quality of deliverables and delay in meeting the deadlines	3,5	Proper internal peer review procedures and criteria will be in place in order to ensure the quality of the deliverables and their preparation in a timely	1	ongoing	1,9	**1,6**
16	Pilot site delayed or not available any more	4,5	Four additional "backup" sites have been prepared to provide the same services at other locations.	1	ongoing	2,1	**2,4**
17	Partner experts are not paid monthly salary nor having their travel reimbursed	4.0	Partner's administration keep pre-funding in its accounts saving for end-of-period 18M and beginning of next period. Coordinator should update administrations duties and explain what to happen when pre-funding is paid out. Coordinator should address partner's PM budget to be used and explain how to reimburse	1	ongoing	2.0	**2.0**
18	Partner is not contributing to tasks according to their budget	3.0	Coordinator follow-up partner on used PM's with contribution from Work Package leaders	2	ongoing	2.4	**0.6**
19	Volunteers at the Greek test site may find the service is intrusive and ask to be removed from the trial	3.2	Trials need to be designed to minimise intrusion and the chance that people will want to withdraws. A larger number of volunteers will be recruited to allow for some to drop out	2	ongoing	2.5	**0.7**

The evaluation according to the Delta Risk criteria leads to the following risks:

- ID 16, Pilot site delayed – this is due to the high likelihood of this event; indeed, we are already planning four alternative pilot sites, should these be needed.
- ID 15, Poor quality of deliverables – the mitigation action, peer review process, is already in place and is described in deliverable D10.1.

4 Ethics Management

4.1 VICINITY Ethical Policy

Ethical, privacy and legal-related issues will be addressed early in VICINITY by the establishment of the EAB and Ethics Helpdesk (to support the EAB) by Month 10 as part of WP10 activities (Task 10.2). The Ethics helpdesk will advise the project on issues of data privacy, potential for infringement of human rights and misuse of developed technologies. The helpdesk will be provided with a clear mandate and is also expected to provide support to the project participants and training on ethical and privacy concerns to the research team at the offset of the project. It will also provide several guidelines and recommendations for the pilot trials (e.g. Ethics Manual, Informed Consent forms for the participants/volunteers, pilot questionnaires, etc.) taking into account European legislation and the National legislation of the countries, in which the pilot application scenarios will take place (Portugal, Norway and Greece).

VICINITY will follow the opinions of various expert committees in the field (e.g. the European group on ethics (EGE) in science and new technologies to the European Commission. In addition, all national legal and ethical requirements of the Member States where the research is performed will be fulfilled. Any data collection involving humans will be strictly held confidential at any time of the research. This means in detail that:

- all the test subjects will be informed and asked to provide their consent to any monitoring and data acquisition process, all the subjects will be strictly volunteers and all test volunteers shall receive detailed information about the trial; what information needs to be gathered and why; how personal information will be handled to prevent risk from unauthorised use.
- no personal or sensitive data will be centrally stored. In addition, data will be scrambled where possible and abstracted in a way that will not affect the final project outcome, to ensure data subject privacy

In addition, Data Subjects will receive details about the project and its use of personal information in their own language:

- a plain-language, easily understandable written description of the project and its goals;
- the planned project progress and the related testing and evaluation procedures;
- advice on any unrestricted disclaimer rights on their agreement.

4.2 Ethics Advisory Board (EAB)

The EAB will scrutinise the research to guarantee that no undue risk for the user, neither technically nor related to the breach of privacy, is possible. Thus, the Consortium shall implement the research project in full respect of the legal and ethical national requirements and code of practice. Whenever authorisations have to be obtained from national bodies, those authorisations shall be considered as documents relevant to the project. Copies of all relevant authorisations shall be submitted to the Commission prior to commencement of the relevant part of the research project. The General Data Privacy Regulation (2016) (GDPR)[4] comes into force in May 2018, but the regulations will be followed from the outset of the VICINITY project.

In preparation to meet future obligation the consortium has established a group, composed of a representative from the DEMO site in Greece, Alexandra Ananika, a representative from two Norwegian DEMO sites, taking into consideration different verticals, Erik Nygaard, and a representative from the PT DEMO site, Natalie Samovich (in combination with her role as EAB chair).

The EAB roles, composition and asks are summarized below. It would consist of a Liaison represented by:

- Natalie Samovich as Chair of the EAB and PT DPO,
- Christoph Grimm as Project Coordinator, Carna Radoijocic as head of the Project Office, and Nigel Wall as Quality Manager,
- Alexandra Ananika, DPO from Greece
- Erik Nygaard - DPO from Norway – representing two Pilot sites.

Broad representation within the EAB and shared scope of focus of the group should ensure compliance to the EU guidebook on Ethics [4] and guidelines related to the General Data Privacy Regulation [5][6][7]

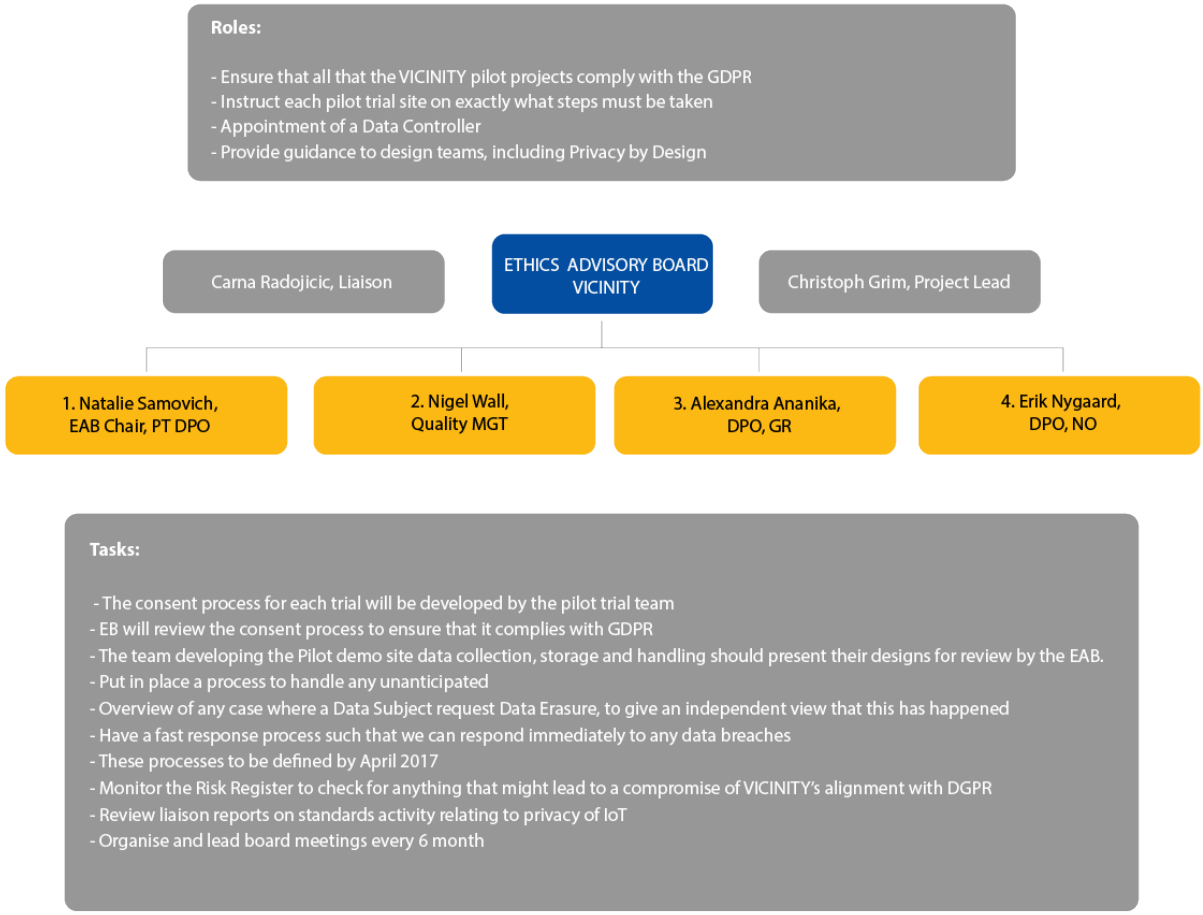

Figure 4-1 Overview of the VICINITY EAB

The EAB shall meet at least at six-monthly intervals – ideally face to face as part of a project coordination meeting, or by teleconference, as required. The EAB has an urgent task to determine the protocol to be followed when the project is required to provide:

- Breach Notification
- Right to Access
- Right to be Forgotten
- Data Portability

Medium term duties (by February 2017) include:

- Provision of guidance to design teams on what must be considered in designing of the VICINITY solutions, to include Privacy by Design criteria.

- Initial guidance to be issued by December 2016.
- The consent process for each trial will be developed by the pilot trial team – the EAB will review the consent process to ensure that it complies with GDPR.
- The team developing the Pilot trial data collection, storage and handling should present their designs for review by the EAB
- The EAB will instruct each pilot trial site on steps they must undertake for design and implementation of the use cases to ensure that all that the VICINITY project considers for implementation will comply with the GDPR.
- The EAB will appoint a Data Controller who will manage the day-to-day use of the data for all pilot sites and Use cases. This role will be considered at the 1st meeting of the EAB.
- The EAB will instruct and supervise all documentation that must be produced for the pilot sites and Use cases.

Longer term duties (April 2017) for the EAB include putting in place:

- A process to handle any unanticipated scenario with an overview of any case where a Data Subject requests Data Erasure, to give an independent view that this has been carried out.
- A fast response process such that it can respond immediately to any data breaches.
- A process to monitor the Risk Register to check for anything that might lead to a compromise of VICINITY's alignment with GDPR.
- A process to review liaison reports on standards activity relating to privacy of IoT.

4.2.1 Ethics Helpdesk

All data subjects will be given advice on how to contact the Ethics Helpdesk. The Ethics Helpdesk will be operated by the VICINITY Project Office. The purpose is to ensure that all queries from the project partners or requests from Data Subjects will be promptly acknowledged and passed to the members of the EAB.

The most urgent action would be if a data breach were to be discovered. Immediate action would be needed to ensure that the authorities are notified if there was any breach of privacy that required formal notification.

4.3 Privacy

Privacy is at the heart of VICINITY's Ethics Policy. We shall follow the AIOTI principles of "privacy by design" in all project work. This includes:

- Minimising the inclusion of personal data in all data processing. Note that the use of a pseudonym (e.g. a unique reference number) instead of a user name helps to obscure data, but that data is still classed as personal data,
- Designing the security of VICINITY'S communications systems "As if they were carrying personal data" even if these communication links do not carry personal data.

  In addition, the privacy approach principle will be followed in accordance with the European book on Ethics in research guidelines in order to ensure that pilot participants will maintain:
  - control over access to their personal information; (addressed in GDPR guidelines)

- information and control over impact to oneself, in both physical and mental ways. This will be addressed at the 1st meeting of the EAB. Guidance will also be sought from the governing body.
- knowledge and control over their ability to make important decisions about family and lifestyle in order to be self-expressive and to develop varied relationships.

4.4 VICINITY's Detailed Data Management Plan

VICINITY will participate in the Open Research Data Pilot [8]. In this context, a detailed data management plan (D9.2) was delivered at Month 6 of the project, fully describing the procedures for ensuring that the data management process complies with National (Portugal, Norway and Greece) and EU Legislation. The following subsections form the draft of that document.

The consortium's approach will be in full compliance with the EU legislative and regulatory framework [3] for data protection based on the uniform approach of EC Directive 95/46/EC3, the European GDPR and the national legislative and regulatory framework for data protection of each project member country (an effort will be given in order to fulfil the specific requirements for data protection of each country within the EU and associated countries like Norway). In general, the VICINITY project does not introduce any critical ethical issues or problems, however several considerations typical to ICT and IoT applications and on-site pilot trials shall be taken into account (see DMP: Section 3.2 IPR management and security). The consortium is fully aware of these and has the necessary experience to address them seamlessly.

Main changes under GPDR and how they differ from the previous directive are listed below. This information has been sourced from [8].

> *"The aim of the GDPR is to protect all EU citizens from privacy and data breaches in an increasingly data-driven world that is vastly different from the time in which the 1995 directive was established. Although the key principles of data privacy still hold true to the previous directive, many changes have been proposed to the regulatory policies; the key points of the GDPR as well as information on the impacts it will have on business can be found below".*

These main difference were identified as relevant to the pilots and EAB will work on providing a roadmap and incorporating theses changes and considerations:

Increased Territorial Scope (extra-territorial applicability).

"Arguably the biggest change to the regulatory landscape of data privacy comes with the extended jurisdiction of the GDPR, as it applies to all companies processing the personal data of data subjects residing in the Union, regardless of the company's location. Previously, territorial applicability of the directive was ambiguous and referred to data process 'in context of an establishment'. This topic has arisen in a number of high profile court cases. GPDR makes its applicability very clear - it will apply to the processing of personal data by controllers and processors in the EU, regardless of whether the processing takes place in the EU or not. The GDPR will also apply to the processing of personal data of data subjects in the EU by a controller or processor not established in the EU, where the activities relate to: offering goods or services to EU citizens (irrespective of whether payment is required) and the monitoring of behaviour that takes place within the EU. Non-EU businesses processing the data of EU citizens will also have to appoint a representative in the EU.

Penalties

Under GDPR organizations in breach of GDPR can be fined up to 4% of annual global turnover or €20 Million (whichever is greater). This is the maximum fine that can be imposed for the most serious infringements e.g. not having sufficient customer consent to process data or violating the core of Privacy by Design concepts. There is a tiered approach to fines e.g. a company can be fined 2% for not having their records in order (article 28), not notifying the supervising authority and data subject about a breach or not conducting impact assessment. It is important to note that these rules apply to both controllers and processors -- meaning 'clouds' will not be exempt from GDPR enforcement.

Consent

The conditions for consent have been strengthened, and companies will no longer be able to use long illegible terms and conditions full of legalese, as the request for consent must be given in an intelligible and easily accessible form, with the purpose for data processing attached to that consent. Consent must be clear and distinguishable from other matters and provided in an intelligible and easily accessible form, using clear and plain language. It must be as easy to withdraw consent as it is to give it.

Data Subject Rights

Breach Notification

Under the GDPR, breach notification will become mandatory in all member states where a data breach is likely to "result in a risk for the rights and freedoms of individuals". This must be done within 72 hours of first having become aware of the breach. Data processors will also be required to notify their customers, the controllers, "without undue delay" after first becoming aware of a data breach.

Right to Access

Part of the expanded rights of data subjects outlined by the GDPR is the right for data subjects to obtain from the data controller confirmation as to whether or not personal data concerning them is being processed, where and for what purpose. Further, the controller shall provide a copy of the personal data, free of charge, in an electronic format. This change is a dramatic shift to data transparency and empowerment of data subjects.

Right to be Forgotten

Also known as Data Erasure, the right to be forgotten entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data, and potentially have third parties halt processing of the data. The conditions for erasure, as outlined in article 17, include the data no longer being relevant to original purposes for processing, or a data subjects withdrawing consent. It should also be noted that this right requires controllers to compare the subjects' rights to "the public interest in the availability of the data" when considering such requests.

Data Portability GDPR introduces data portability - the right for a data subject to receive the personal data concerning them, which they have previously provided in a 'commonly use and machine readable format' and have the right to transmit that data to another controller.

Privacy by Design

Privacy by design as a concept has existed for years now, but it is only just becoming part of a legal requirement with the GDPR. At its core, privacy by design calls for the inclusion of data protection from the onset of the designing of systems, rather than an addition. More

specifically: "The controller shall implement appropriate technical and organisational measures .in an effective way. in order to meet the requirements of this Regulation and protect the rights of data subjects". Article 23 calls for controllers to hold and process only the data absolutely necessary for the completion of its duties (data minimisation), as well as limiting the access to personal data to those needing to act out the processing.

Data Protection Officers
Currently, controllers are required to notify their data processing activities with local DPAs, which, for multinationals, can be a bureaucratic nightmare with most Member States having different notification requirements. Under GDPR it will not be necessary to submit notifications / registrations to each local DPA of data processing activities, nor will it be a requirement to notify / obtain approval for transfers based on the Model Contract Clauses (MCCs). Instead, there will be internal record keeping requirements, as further explained below, and DPO appointment will be mandatory only for those controllers and processors whose core activities consist of processing operations which require regular and systematic monitoring of data subjects on a large scale or of special categories of data or data relating to criminal convictions and offences. Importantly, the DPO:

- Must be appointed on the basis of professional qualities and, in particular, expert knowledge on data protection law and practices
- May be a staff member or an external service provider
- Contact details must be provided to the relevant DPA
- Must be provided with appropriate resources to carry out their tasks and maintain their expert knowledge
- Must report directly to the highest level of management
- Must not carry out any other tasks that could result in a conflict of interest." [8].

The EAB will issue guidance on what needs to be done to comply with GDPR guidelines and requirements to pilot sites and in collaboration with DPOs.

In order to replicate the pilots configuration, test pilot sites will be established. They will incorporate methods and equipment that reflects the other pilot installations. This means that the table structure and safety measures will be similar, but with other test data. These pilot sites will not gather or generate personal information, but will offer insights into best practice and identify potential issues with the approach.

The further handling of datasets gathered through the four different test domains, will be identified through the two next DMP deliverables; D9.3 due in M24 and D9.4 due in M36. These deliverables will further explore appropriate collection and publication of data expanding on datasets and, and look into reuse of architecture and secure integration.

4.4.1 Data to be collected within VICINITY Pilot Use Cases

Data will be automatically collected by IoT sensors and other proprietary equipment installed at selected pilot areas during the execution of the 4 envisaged pilot Use Cases, as described in *Section 1.2.2* of the Project Proposal and will be further investigated in T1.2 (*Pilot Sites Surveys and extraction of Use Case requirements*) and respective tasks of pilot deployment (WP7) and pilot realisation (WP8). In most cases the collected data will be data needed for monitoring the contextual conditions of the pilot areas (devices consumption, energy production, traffic, temperature, weather etc.). In some cases, some of the collected data will be related to the actual end-users (such as inhabitants of assisted living buildings, elderly people participating in the eHealth Use Case etc.). Therefore, since some of the collected

data in the latter case may involve sensitive personal data, all provisions for data management will be made in compliance with National and EU legislation, as described in the following paragraphs.

4.4.2 Data Collection and Storage Methodology

Overall, data will be stored in secure server systems and will be anonymized. Only the project coordinator (UNIKL) and selected personnel from lead pilot partners (ENERC, TINYM, HITS and MPH) will possess the key to re-identification. No personal information or data that can identify individual pilot participants (such as inhabitants of assisted living buildings, elderly people participating in the eHealth Use Case etc.) will be collected and stored. Instead, all pilot participants will be assigned a unique ID based on each participant's role in each of the pilot use case (role ID). This will open for aggregating personal data without revealing the associated user. It will additionally allow mapping of participants' actions during the use case execution and pilot realisation phase, creating an opening for generating context sensitive information. The relationship between the role ID and the participant will be recorded at the repository and will be stored separately and securely. This file will be accessible only to the corresponding leader of each of the pilot trials. The relationship between database tables containing participants personal information and data being gathered will not be provided to anyone, thus adhering to the EU regulations on data privacy. Furthermore, data will be kept for the least period of time necessary to accomplish the goals of the project and the population of the VICINITY Repository. In any case, all data that will be considered confidential from the trials will be discarded by the project completion, whereas only the public models and respective datasets that will be described in details in the Data Management Plan will be kept open.

4.4.3 Data protection

In order to protect the collected data and control unauthorised access to the VICINITY data repositories, a separate task (T4.3 VICINITY Security Services) will be devoted in ensuring security and protection of the VICINITY components, utilizing state of the art processes and tools in terms of authentication and encryption services. Furthermore, only authenticated personnel will have access to pilot-specific data collected. During the proposed system lifecycle, a holistic security approach will be followed, in order to protect the pillars of information security (confidentiality, integrity, availability) from a misuse perspective. The security approach will be identified by a methodical assessment of security risks followed by their impact analysis. This analysis will be performed on the personal information and data processed by the proposed system, their flows and any risk associated to their processing.

Towards the protection of personal data of volunteer pilot participants, the following issues will be taken into account:

- All data associated with a recognizable person will be held private.
- Individual data on subjects will be used in strictly confidential terms and will only be published as statistics (anonymously).
- Any data or information about a person will be held private, regardless of how this data was acquired. Therefore, data obtained incidentally within VICINITY project will be handled with confidentiality. This accidental obtainment does not substitute the compulsory procedure, in which researchers need each participant's explicit consent to obtain, store and use information about them.
- All individual information will be anonymised (or coded) in full and at the earliest possible point in time during data processing.

- Data should be stored in a secure location and not shared with physical media like USB flash drives.

During the VICINITY project, responsibilities will be clearly assigned for the overall management and control of research findings and the controlling of access rights. The person who will be responsible on issues for data security will directly inform to the quality board, the ethics helpdesk and the project coordinator.

4.4.4 Data retention and destruction

Within the VICINITY Data Management Plan, the open research data retention and destruction strategy will be also reported along with the limits on their secondary use and their disclosure to third parties. A number of critical factors that are relevant for data retention will be taken into account, namely:

i) *Purpose of retaining data,*
ii) *Type of open data collected,*
iii) *Policy access to the open data,*
iv) *data storage, security and protection measures and*
v) *Confidentiality and anonymity of data. Regarding data destruction, as computerized data (hard disk drives) will be used for data storage, existing methods for permanent and irreversible destruction of the data will be utilized (i.e. full disk overwriting and re-formatting tools).*

In all cases the data protection and privacy of personal information will be governed by the following principles, which consist of part of an overall information security policy:

- Protective measures against infiltration will be provided
- Physical protection of core parts of the systems and access control measures will be provided
- Logging of VICINITY system and appropriate auditing of the peripheral components will be available.

4.4.5 Measures for preventing malevolent/criminal/terrorist abuse of research findings

During the VICINITY project, responsibilities will be clearly assigned for the overall management and control of research findings and the controlling of access rights. The person who will be responsible on issues for data security will directly inform to the quality board and the project coordinator. The research findings will be protected from malevolent/criminal/terrorist abuse by following strictly procedures, as they will be defined by the EAB.

4.4.6 Pilot Participant Recruitment Process for the execution of the Pilot Use Cases

The VICINITY pilot use case trials will involve existing habitants/employees/residents of selected buildings in each of the selected pilot areas (such as assisted living buildings in Norway) along with volunteers wishing to participate in some of the envisioned pilot use cases (for example people with hypertensive, dementia or obesity in the eHealth Use Case in Greece). All people that will be actively participating and/or being affected by the execution of each of the pilot use case, will take part in a thorough recruitment and informed consent procedure, that will be particularly stringent to ensure no coercion (not even soft or indirect) is exerted. The specific criteria for the selection of the volunteer participants will be determined by the pilot requirements, while there will be participants with various roles as described in the use cases of the project. In the case of the Greek pilot, the relatives of the elderly should also be contacted and their information gathered.

Furthermore, specific measures to protect the participants from a breach of privacy/confidentiality and potential discrimination will be applied, as it follows:

- Confidentiality: The names of the people participating in the trials will never be revealed in any document and their participation will not be communicated to other pilot participants. As already stated above, all personal data stored during the pilot trials will be completely and irreversibly anonymised and will be erased at the completion of the VICINITY Project. As an absolute minimum anonymised process, data will not contain any of the following, or codes for the following:
    - Name, address, phone/fax. number(s), e-mail address, full postcode
    - Any identifying reference numbers, photographs, information about relatives
- Right to get more information about the trials: the pilot participants will be able to ask any questions about the pilot trials at any time throughout the pilot realisation phase. The corresponding pilot trial responsible partner will be available to answer any questions, interests or concerns about the pilot trial executions. During the pilot trials execution, each of the pilot participants will have the right to withdraw from the trials at any time, without having to give any explanation and without being affected in any way. Data Subjects may also ask for removal of all historical data that can be linked to them.

Informed Consent: A detailed informed consent will be carefully prepared for each pilot trial, fully outlining the scope of the Trial and its purposes along with the data collected and analysed.

4.4.7 Methodology & Guidelines for the delivery of Informed Consent

The consent procedures will be carefully determined and managed by pilot-specific tasks (T8.2, T8.3 and T8.4) that will manage the trials which will be performed in selected pilot areas. Thus, it will require the enrolment of people voluntarily declaring their consent to participate in each of the pilot use cases. However, the design of the observational study will be prepared in strict collaboration with the EAB, in order to respect privacy and ethical issues implied by the data to be collected and analysed. In particular, the consortium will take the appropriate action that:

1. No data can be collected without the explicit informed consent of people under observation no person that is unable to express a free and informed consent for age-related reasons, ongoing medical and / or psychological conditions, mental incapacity, will be enrolled in the study;
2. No data collected may be sold or used for any different purposes from the VICINITY project;
3. Only data, which is strictly necessary to accomplish the current study, will be collected; data minimisation will be applied at every level possible and will be supervised by the EAB of the project.
4. The use of shadow (ancillary) personal data will be minimised in the course of the observation: any collected data shall be deleted as soon as possible. Special attention will be also paid to comply with Council of Europe's Recommendation R(87)15 on the processing of personal data for police purposes, Art.2 : "The collection of data on individuals solely on the basis that they have a particular racial origin, particular religious convictions, sexual behaviour or political opinions or belong to particular movements or organisations which are not proscribed by law should be prohibited. The collection of data concerning these factors may only be carried out if absolutely necessary for the purposes of a particular inquiry". The EAB does not believe that there should be any justification for acquiring any such data within the VICINITY project.

The consent procedure for the pilot use case realisation at each of the selected pilot sites will be obtained through a two stage procedure:

a. Initially the pilot trial's leader will orally present the pilot to people that will be involved, carefully describing the level of privacy infringement that the execution of each of the pilot realisation involves. In case someone wants to exercise his/her right not to know, he/she will be excluded from the pilot.
b. Secondly, after a few days, subjects will be required to read and sign an informed consent form that will explain in both plain English and in local language what the trial leader has already orally explained. The informed consent forms in English and in local language to be used will be sent to the European Commission and included in the experimental protocol.

A template of such a consent form, to be adopted as required per pilot use case, is provided in Annex B.

5 Conclusions

This document provides information on two important aspects of the VICINITY management process:

- This document has presented the approach that is being taken for the management of Risk and Contingency planning, using the Extended Failure Mode and Effect Analysis (EFMEA) technique.
- The risks are identified, characterised and mitigation plans recorded using a Risk Register. The risk register shown in the document has been reviewed but will change as the project progresses, so it is important to always use the latest Risk Register which can be found at: https://cpsgw.cs.uni-kl.de/cpscloud/index.php/apps/files/?dir=%2FVICINITY4Consortium%2FRisk%20Register
- EFMEA has been chosen following a review of the alternative approaches, and its operation has been explained.
- The constitution, responsibilities and operation of the EAB has been described. A number of specific questions and actions have been identified as a starting point for the EAB
- The quality management board will review the operation of the processes described in this document and may call for these to be revised in the light of operational experience.

6 References

[1] http://www.vicinity-h2020.eu

[2] ICT 30 – 2015: Internet of Things and Platforms for Connected Smart Objects - http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/topics/914-ict-30-2015.html

[3] European Regulation: General Data Protection Regulation (May 2016) http://www.eugdpr.org/the-regulation.html

[4] https://ec.europa.eu/research/science-society/document_library/pdf_06/textbook-on-ethics-report_en.pdf

[5] https://iapp.org/resources/article/top-10-operational-impacts-of-the-gdpr/

[6] http://www.eugdpr.org

[7] http://www.eugdpr.org/more-resources-1.html

[8] Open Data Research Data Pilot; https://www.openaire.eu/opendatapilot

[9] GDPR interpretation Key changes document: http://www.eugdpr.org/the-regulation.html

[10] EN2900 = ISO 9001, based on BS 5750 "Quality Management Systems" Standard.

[11] Zigmund Bluvband, Pavel Grabov, Oren Nakar: "Expanded FMEA (EFMEA)". Reliability and Maintainability, 2004 Annual Symposium – RAM. IEEE 2004. DOI: 10.1109/RAMS.2004.1285419

Annex A: Risk Register Template

Risk Register for VICINITY Project

Date 15/02/2016 Version number 0.1 Status:

ID	type	WP	Risk event	Impact	origin	Prob'lity	Consq'ces	Risk	Mitigation Action Plan	Owner	Feasi-bility	Risk After	Delta Risk
						Note 1	Note 2	Note 3					
1													
2													
3													
4													
5													
6													
7													
8													
9													
10													

Note 1: High = 5, Low = 1
Note 2: High = 5, Low = 1
Note 3: Risk = Probability x Consequences

Annex B: Participant Consent Form Template

VICINITY 2020

Consent Form

Purpose of the study

A plane-language easily understandable written description of the project and its goals (2-3 paragraphs)

Planned Project Progress

The planned project progress and the related testing and evaluation procedures (1-2 paragraphs)

Disclaimer Rights

Advice on unrestricted disclaimer rights on their agreement.

Voluntary Participation Form for the needs of the VICINITY project

1. Participant Information

Basic information and participant's reference code ID (the reference code ID will be used throughout the pilot trial execution)

2. Study Information

Details about the pilot Use Case

3. Participant's Questionnaire

Questions verifying that the participant:

- has been fully informed on the purpose, duration, procedures of the study;

- has been informed on the rights to deny participating or to quit from the study and about the corresponding consequences.

- has been informed on the contact person in case that he/she has questions and queries about the study.

- had adequate time to take a decision concerning his/her participation in the study.

- comprehend that he/she can quit from the study at any time without having to justify his/her decision.

- has been informed about potential effects, difficulties and dangers.

- has been informed about the sensors equipment that will be used to collect data.

- has been informed about the security of the study data and results.

- has been ensured about the confidentiality of his/her personal information. Publications of the study results do not allow the personal data recognition, due to the principle of anonymity. Always under the confidentiality principles.

4. Signed Consent to Participate

A signed consent of the participant allowing the study responsible to examine and inspect the data collected during the study.