

H2020 Project: Smart Resilience Indicators for Smart Critical Infrastructure

D7.1 - Ethics Protocol



Coordinator: Aleksandar Jovanovic EU-VRi

Project Manager: Bastien Caillard EU-VRi

European Virtual Institute for Integrated Risk Management
Haus der Wirtschaft, Willi-Bleicher-Straße 19, 70174 Stuttgart

Contact: smartResilience-CORE@eu-vri.eu

Ethics Protocol



Report Title:	<i>Ethics Protocol</i>		
Author(s):	Brauner, F.; Fiedrich, F.		
Responsible Project Partner:	BUW	Contributing Project Partners:	EU-VRI

Document data:	File name / Release:	SmartResilience-D7.1-EthicsProtocols_v03bc31102016		Release No.: 1
	Pages:	18	No. of annexes:	1
	Status:	Final	Dissemination level:	PU/CO
Project title:	SmartResilience: Smart Resilience Indicators for Smart Critical Infrastructures		Grant Agreement No.:	700621
			Project No.:	12135
WP title:	Ethics Protocol		Deliverable No:	D7.1
Date:	Due date:	October 31, 2016	Submission date:	October 31, 2016
	Keywords: Ethics, protocols, safety, privacy, legality, authorization, protection, environmental data, personal information			
Reviewed by:	Frank Fiedrich (as Ethics controller)		Review date:	October 26, 2016
	Neelke Doorn (as Ethics advisor)		Review date:	October 26, 2016
	Bastien Caillard		Review date:	October 28, 2016
Approved by Coordinator:	A. Jovanovic		Approval date:	October 31, 2016

Wuppertal, October 2016



Release History

Release No.	Date	Change
1	October 26, 2016	Draft for reviewers
2	October 31, 2016	Version submitted

Project Contact



EU-VRI – European Virtual Institute for Integrated Risk Management
Haus der Wirtschaft, Willi-Bleicher-Straße 19, 70174 Stuttgart, Germany
Visiting/Mailing address: Lange Str. 54, 70174 Stuttgart, Germany
Tel: +49 711 410041 27, Fax: +49 711 410041 24 – www.eu-vri.eu – info@eu-vri.eu
Registered in Stuttgart, Germany under HRA 720578

SmartResilience Project

Modern critical infrastructures are becoming increasingly smarter (e.g. the smart cities). Making the infrastructures smarter usually means making them smarter in the normal operation and use: more adaptive, more intelligent etc. But will these smart critical infrastructures (SCIs) behave smartly and be smartly resilient also when exposed to extreme threats, such as extreme weather disasters or terrorist attacks? If making existing infrastructure smarter is achieved by making it more complex, would it also make it more vulnerable? Would this affect resilience of an SCI as its ability to anticipate, prepare for, adapt and withstand, respond to, and recover? What are the resilience indicators (RIs) which one has to look at?

These are the main questions tackled by SmartResilience project.

The project envisages answering the above questions in several steps (#1) By identifying existing indicators suitable for assessing resilience of SCIs (#2) By identifying new smart resilience indicators including those from Big Data (#3) By developing, a new advanced resilience assessment methodology based on smart RIs and the resilience indicators cube, including the resilience matrix (#4) By developing the interactive SCI Dashboard tool (#5) By applying the methodology/tools in 8 case studies, integrated under one virtual, smart-city-like, European case study. The SCIs considered (in 8 European countries!) deal with energy, transportation, health, and water.

This approach will allow benchmarking the best-practice solutions and identifying the early warnings, improving resilience of SCIs against new threats and cascading and ripple effects. The benefits/savings to be achieved by the project will be assessed by the reinsurance company participant. The consortium involves seven leading end-users/industries in the area, seven leading research organizations, supported by academia and lead by a dedicated European organization. External world leading resilience experts will be included in the Advisory Board.

Executive Summary

The purpose of this document is to state potential ethical issues of the research project SmartResilience and to provide ethical guidelines, which have to be followed by each research partner of the project.

These guidelines shall ensure that matters of safety, privacy, legality, authorization, protection, ethics and general conduct regarding environmental data, personal information and research results are considered and implemented properly in the research process.

Researchers have overall responsibility for ensuring that research is carried out in accordance with these guidelines, and for ensuring that clients and other parties to the research agree to comply with its requirements.

Table of Contents

Release History	i
Executive Summary	iii
List of Tables	v
List of Acronyms	vi
1 Introduction	7
2 Ethical Concerns	8
2.1 Preamble and “Code of Conduct”	8
2.2 Ethics Committee	9
2.3 Research on Humans	9
2.3.1 Informed Consent	10
2.3.2 Informed Consent for the Use of Pre-existing Data	10
2.4 Privacy	11
2.5 Data Protection	11
2.5.1 Use of Data	11
2.5.2 Misuse & Security of Data Processing	11
2.6 Professional Responsibility	12
2.6.1 Transparency	12
2.6.2 Honesty	12
2.6.3 Consideration of Gender Aspects	12
2.7 Publishing Findings	13
3 Effective Controlling	14
References	15
A N N E X E S	16

List of Tables

Table 1:	Points raised by reviewers and author's response.....	17
----------	---	----

List of Acronyms

<i>Acronym</i>	<i>Definition</i>

1 Introduction

The SmartResilience project will touch on issues in human research ethics by collecting data from respondents from European countries via a range of activities:

- Engagement measures
- Interviews and survey
- Critical Infrastructure Advisory Board
- Case studies

SmartResilience will conduct surveys and interviews in order to gain a detailed understanding of smart technologies and their role in ensuring resilience of infrastructures, in particular with respect to challenges for Smart City infrastructures regarding different types of threats. Through standardized questionnaires and expert interviews scientific experts as well as operators of critical infrastructures will provide valuable information on vulnerabilities and consequences of typical threats for specific types of infrastructures.

SmartResilience primarily focuses on publicly available data, to respect privacy and data protection expectations.

Both information obtained in the formulation of the SmartResilience concept and the potential outcomes of the project may give rise to ethical and legal implications across different jurisdictions. Therefore, because of the nature of the source material, it is crucial to consider the ethical and legal implications of the project activities. This includes matters of privacy, legality, authorization, protection, ethics and general conduct regarding environmental data, personal information and research results.

All activities of the project will be carried out according to the ethical standards and guidelines of Horizon2020, which will be rigorously applied, regardless of the country in which the research is carried out. With specific relation to national ethical requirements, where appropriate, SmartResilience will not proceed without approval from the national data protection authorities of the countries in which the interviews, surveys and workshops will be conducted.

The project will work in full accordance with the EU Directive 95/94/EC on Data Protection (Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data), the EU Directive 2002/58/EC on privacy and electronic communications (Directive concerning the processing of personal data and the protection of privacy in the electronic communications sector) and their national legal implementations.

In addition to the Ethics Controller of SmartResilience, the project consortium appoints an external and independent Ethics Advisor (see Chapter 2.2) and a Security Officer to create an Ethics Committee.

2 Ethical Concerns

2.1 Preamble and “Code of Conduct”

Researchers shall conform to all relevant national and international laws. In addition, the researchers shall hold paramount the safety, health and privacy of the public.

The rights of respondents as private individuals shall be respected by researchers and they shall not be harmed or adversely affected as the direct result of cooperating in the research project.

Researchers shall ensure that projects and activities are designed, carried out, reported and documented accurately, transparently and objectively. They are bound to the best possible standards in research, doctrine and other professional practice. When researchers give professional judgements, they should state their (professional) knowledge, their methods and experiences in an appropriate and clear way.

Research shall be legal, honest, truthful and objective and be carried out in accordance with appropriate scientific principles.

Researchers have overall responsibility for ensuring that research is carried out in accordance with this Code, and for ensuring that clients and other parties to the research agree to comply with its requirements.

Subsequent correction and/or appropriate redress for a contravention of the Code, by the party responsible, is desirable but does not excuse the contravention.

The Code and the principles enshrined in it, should be adopted and implemented, nationally and internationally, by the relevant local, national or regional self-regulatory bodies. The Code should also be applied, where appropriate, by all organisations, companies and individuals involved and at all stages in the research project.

The SmartResilience project partners are committed to:

- The use of proper scientific methodology;
- Protection of confidentiality (no access other than as statistical aggregates);
- Integrity of the consortium data (ethical responsibility to resist threats to integrity such as political instructions to manipulate concepts etc.);
- Adoption of copying and prevention strategies to ameliorate any potential ethical concerns;
- Achieving an appropriate benefit/burden balance (the scientific advance envisaged through SmartResilience will be significant. However social, human and cultural impacts have also been considered in choices;
- Personal data protection - the processing (obtaining, holding and disclosing) of personal data such as health information, criminal justice, financial information, genetic information and location-based information will not be a central focus in the delivery of the project, and appropriate precautionary mechanisms will be devised to safeguard any instance of data processing.
- Scientific misconduct includes (negligent or intended) fabrication (making up data or results), falsification (changing or misreporting research data or improper manipulation of experiments) and plagiarism (using ideas or words without accurate reference).
- In terms of the above accurate reference means reference fulfilling standards generally used in scientific society for citation or other bibliographic reference
- Principle of voluntariness: choice of participation shall be made of the participant’s free will.

- Principle of selflessness: every participant in the research shall enjoy access rights to the result of another participant in the same action if those results are needed by the former to exploit its own results.
- Principle of due diligence: every participant shall take proper measures to carry out all tasks in a due manner as usual in scientific community and business life and to take every measure in its capacity to avoid causing any misconduct, damage, loss or harm.
- Principle of trust: results of current research shall not be abused or transferred to criminal groups or used to support any kind of unlawful activity, its solely purpose shall be to enhance the security of the citizens.
- Principle of open resource: results of current research shall be disseminated publicly in the European Union and third country members of the Consortium, excluding those which are not allowed for dissemination by data protection rules.
- Principle of detachment: research activities, results and publication may only be based on unbiased, clear facts and logical conclusions without any form of preconceptions or any other approach may result in discrimination.
- Principle of neutrality: Any form of discrimination is strongly prohibited in the whole project!

2.2 Ethics Committee

The role of the Ethics Committee is to ensure the efficacy of the Ethics Code and support the participants to reach the highest ethical standards during the project.

Ethics Committee is a body tasked with

- prevention of scientific misconduct or violation of Ethical Code
- provide guidelines, best practice and other support (forms, case-by-case evaluation) to the participants in connection with fulfilling the obligations set in the Ethics Code
- monitors activity of participants to enforce Code of Ethics and maintain level of data protection;
- carries out periodic ethics assessment annually
- contributes to periodic reports and the final report in scope of ethics and data protection
- investigates cases connected to possible scientific misconduct, violation of Ethics Code, other damage or loss caused by participants to the Consortium or to third parties

The Ethics Committee is functioning during the entire duration of the project and it consists of:

- a. an Internal Ethics Advisor (Chairman) = Prof. Dr. Frank Fiedrich
- b. an External Ethics Advisor = Dr. mr. ir. Neelke Doorn
- c. Security Officer (if necessary) = Dr. Zoltán Székely from Hungarian National Police

The Chairman summons the Committee and chairs the sessions. The External Ethics Advisor is an independent person contracted by the consortium, supervises the application of the Code of Ethics. His/her activity includes counselling (if necessary) and auditing (for further information, please see contract). The Security Officer is tasked to maintain level of data protection. This activity will be embedded in project quality management. The Ethics Committee shall resolve every case with a written decision within 30 days.

2.3 Research on Humans

Respondents' cooperation is entirely voluntary at all stages and must be based on adequate, and not misleading, information about the general purpose and nature of the project when their agreement to participate is being obtained and all such statements shall be honoured.

For all activities in the project, it is planned to use mentally competent adults, which means that they will be in a position to understand their role in the project.

Rights of the respondent

Appropriate measures shall be taken to ensure that respondents understand and can exercise their rights:

- not to participate in the research project;
- to withdraw from the research project at any time;
- to require that their personal data are not made available to others; and
- to delete or to rectify incorrect personal data which are held on them.

All aspects of the methods used (including informed consent forms etc.) are developed in order to ensure that the participants have knowledge about:

- that participation is voluntary
- that they can ask questions and receive understandable answers before making a decision
- the degree of risk and burden involved in participation
- who will benefit from participation
- assurances that appropriate insurance cover is in place
- that they can withdraw themselves and their data from the project at any time
- any potential commercial exploitation of the research

2.3.1 Informed Consent

Informed consent is mandatory. Participants in interviews or other activities have to be asked to sign an 'informed consent form'. This form describes what the collected information will be used for and how the participant can review this information – and, if necessary, ask for correction or deletion.

Participants have to be informed detailed and correctly about the objectives and methods of the research and that they participate on a voluntary basis. It is the participants' right to change their mind and to withdraw themselves and their data from the research, also after giving informed consent, at any time of the research process.

Measures to protect the privacy of participants in data collection will be described to participants by means of the Informed Consent Form and by an accompanying Project Information Sheet that explains the objectives of the project, and the motivation for the interaction. Before any interaction can commence, the participants will need to have given their confirmation of their understanding of these measures and consent for use of data stemming from the interaction by signing the Informed Consent Form.

For some specific research activities, it may be required that research participants do not receive detailed information about the aim and the set-up of the specific research activity, because that would distort the results. The fact that some information is withheld from the participants requires explicit approval from the ethic commission.

In the IC procedure, participants are explicitly informed about the possibility that some information may be withheld for the sake of the activity. Information about potential safety, health, or privacy issues will not be withheld.

In case of an interview with multiple participants (e.g. a workshop or a discussion forum), all participants are required to sign an Informed Consent Form.

The participant should be given a copy of his signed Informed Consent Form.

Each consortium partner conducting an interview is responsible for securing the signed Informed Consent Form, and storing it in a secure location for possible future verification and use.

2.3.2 Informed Consent for the Use of Pre-existing Data

During the course of the research, it is possible that the SmartResilience team will gain access to data that was collected before the start of the project, by an organisation who is not a member of the consortium. In this event, the SmartResilience partner who receives this data must ensure that there is no information contained in the data that could be used to identify individual citizens. Further, the SmartResilience partner

must be mindful of the risks of linking this data, or conclusions resulting from this data with data or conclusions from other data sources.

In a similar way as when interacting with human participants, informed consent must be obtained when acquiring pre-existing data from external sources.

This procedure is not necessary when data has been explicitly released to the public domain, or released under clearly stated conditions that include the intended usage within the SmartResilience project.

2.4 Privacy

The identity of respondents has to be protected and will not be revealed to the user of the information without explicit consent.

Respondents shall be informed before observation techniques or recording equipment are used for research purposes, except where these are openly used in a public place and no personal data are collected. If respondents do wish so, the record or relevant section(s) of it shall be destroyed or deleted. In the absence of explicit consent respondents' personal identity shall be protected.

When collecting genetic information or personal data (e.g. health, sexual lifestyle, ethnicity, political opinion, religious or philosophical conviction) from respondents, researchers shall ensure that respondents are aware of the purpose of the collection and respondents are aware of any quality control activity involving re-contact.

2.5 Data Protection

2.5.1 Use of Data

Personal information collected and held in accordance with these guidelines shall be:

- collected for specified research purposes and not used in any manner incompatible with these purposes;
- adequate, relevant and not excessive in relation to the purpose of the research for which they are collected and/or further processed;
- and preserved no longer than is required for the purpose for which the information was collected or further processed.

Researchers shall ensure that respondents' personal identity is withheld from the client. The researcher may communicate the respondent's identifiable personal information to the client, unless national provisions require stricter regulations, under the following conditions:

- the respondent has explicitly expressed this wish and/or
- the respondent has given their explicit consent and
- on the understanding that no commercial activity will be directed at them as a direct result of their having provided information.

2.5.2 Misuse & Security of Data Processing

It is essential to prevent unauthorised access and also to control issues such as ability to edit material.

Researchers shall never allow personal data that they collect in a research project to be used for any other purpose.

Protection of confidentiality has to be guaranteed: No access other than as statistical aggregates. If there is a need for exceptions, these will not take place without the explicit consent of the participant.

Researchers shall ensure that adequate security measures are employed in order to prevent unauthorised access, manipulation to or disclosure of the personal data.

If personal data are transferred to third parties, it shall be established that they employ at least an equivalent level of security measures.

Particular care shall be taken to maintain the data protection rights of individuals when personal data are transferred from the country in which they are collected to another country.

When data processing is conducted in another country, all reasonable steps shall be taken to ensure that adequate security measures are observed and that the data protection principles of this Code are respected.

Researchers shall inform clients, prior to work commencing, when any part of the work for them is to be subcontracted outside the researchers' own organisation (including the use of any outside consultants). On request clients shall be told the identity of any such subcontractor.

A differentiation between unprocessed, processed and public data should occur. Unprocessed data is data that is captured by individual consortium partners, and that might contain personal information. Processed data is data that is shared among the consortium, and that does not contain any personal information. Public data is data that is based upon processed (consortium-shared) data, but presented to the public at an aggregated level.

No automatic data collection or data collection without project-related intent can be used as a strategy to ensure security of data processing. Data collection activities in the project should be limited on the research scope/objectives, not done in an automatic fashion, and only done with justifiable project-related cause.

2.6 Professional Responsibility

Researchers shall take all reasonable precautions to ensure that respondents are in no way harmed or adversely affected as a direct result of their participation in the research project (interview, experiment, observation, data analysis etc.) especially in the case studies.

Participants have to be informed about all risks, which exceed the ordinary risks in daily life. The anonymity of the participants has to be maintained.

Researchers shall take special care when interviewing children and young people. The consent of the parent or responsible adult shall first be obtained before interviewing children.

Persons, which are physically or mentally not able to give consent to their participation in the research project, have to be respected and excluded of the recruiting process.

2.6.1 Transparency

Researchers shall promptly identify themselves and unambiguously state the purpose of the research.

Respondents shall be able to check the identity and bona fides of the researcher without difficulty.

Researchers shall on request allow the client to arrange for checks on the quality of data collection and data preparation.

Researchers shall provide their clients with appropriate technical details of any research project carried out for the clients.

Researchers shall ensure that research projects are designed, carried out, reported and documented accurately, transparently and objectively.

2.6.2 Honesty

Research shall not abuse the trust of respondents or exploit their lack of experience or knowledge.

Researchers shall not make false statements about their skills, experience or activities, or about those of their organisation.

2.6.3 Consideration of Gender Aspects

The SmartResilience project will not create any particular gender or equal opportunity issues. Principle equal rights will be respected in, during, and following the project for all legal entities and physical persons irrespective of sex, age, race, gender, handicap and nationality.

2.7 Publishing Findings

Where any of the findings of the research project are published, the coordinator shall be asked to consult the researcher in form and content of ethical concerns of the findings.

The project partners have a responsibility to ensure that published results are not misleading and that no important research results are left out. Details about theories, methods and the research concept, which are required to interpret the research results and their limitations in a reasonable way, have to be provided to the best of the researchers' knowledge.

When reporting on the results of the research project, researchers shall make a clear distinction between the findings, the researchers' interpretation of these findings, and any recommendations based on them.

Researchers shall always be prepared to make available the technical information necessary to assess the validity of any published findings.

3 Effective Controlling

In the very beginning of the project, the project-internal Ethics Controller consulted with all partners to determine where precisely the project may involve ethical considerations (e.g., relating to any primary research and stakeholder data collection). Upon this consultation, this internal protocol for ethical procedures has been compiled for the consortium to follow.

Throughout the duration of the project, the Ethics Controller organizes the internal monitoring of the implementation of the ethical protocol by the consortium. The evaluation of this monitoring will be reported in the interim and final reports of the project.

BUW leverages partners' existing expertise in ethical research methods by undertaking internal ethical monitoring activities. This exercise began with the compilation of this ethical protocol for the project, which focuses on the ethical procedures for the consortium to follow with regards to ensuring adequate ethical standards are met and that data protection measures are taken and will include informed consent and information sheet documents. All partners will be requested to review this document and sign a letter of intent for following the protocol throughout the project. Throughout the duration of the project, BUW will monitor and evaluate the implementation of the ethical protocol by all partners. If necessary, this document will be revisited and revised if any additional ethical issues arise. All issues pertaining to ethics approval will be forwarded to SmartResilience's Steering Committee for notification and approval. The evaluation of the monitoring exercise and ethical practices of the project will be reported during the interim and final review.

The Ethics Advisor will evaluate the ethics compliance in the deliverables (for further information please see contract) that will be submitted together with the Periodic Reports to the European Commission. The report (responsible is the Ethic Controller) will consist of the assessment of the proper implementation of ethical standards and guidelines of Horizon2020 and provide sufficient information on ethical or other issues arising from the ethical screening.

If any ethical issues or challenges arise please contact on a primary basis the Ethics Controller Prof. Dr. Frank Fiedrich and secondary the Ethics Advisor Dr. Neelke Doorn:

Ethics Controller:

Univ.-Prof. Dr.-Ing. Frank Fiedrich

Mail: Fiedrich@uni-wuppertal.de

Phone: +49 202 31713 280

Ethics Advisor:

Dr. mr. ir. Neelke Doorn

Mail: N.Doorn@tudelft.nl

Phone: +31 15 27 88059

References

- [1] Ammicht Quinn, Regina; Nagenborg, Michael; Rampp, Benjamin & Wolkenstein, Andreas F.X. (2014): Ethik und Sicherheitstechnik. Eine Handreichung. In: Ammicht Quinn, Regina (Hg.): Sicherheitsethik. Wiesbaden: Springer VS, p. 277-296.
- [2] Ethikkommission DGP e.V. (2014): Ethik-Kodex der Deutschen Gesellschaft für Soziologie (DGS) und des Berufsverbandes Deutscher Soziologinnen und Soziologen (BDS). http://www.soziologie.de/fileadmin/_migrated/content_uploads/Ethik-Kodex_2014-06-14.pdf
- [3] EU Directive 95/94/EC on Data Protection - Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data
- [4] EU Directive 2002/58/EC on privacy and electronic communications - Directive concerning the processing of personal data and the protection of privacy in the electronic communications sector
- [5] Flick, Uwe; Von Kardorff, Ernst & Steinke, Ines [Hg.] (2012): Qualitative Forschung. Ein Handbuch. Hamburg: Rowohlt Taschenbuch Verlag, p. 588-600.
- [6] HARMONISE Project (2012): Appendix I. p..1-5.
- [7] HARMONISE Project (2012): Part B. Description of Work – Ethics Issues. S. 74-79.
- [8] ICC/ESOMAR (2007): International Code on Market and Social Research. https://www.esomar.org/uploads/public/knowledge-and-standards/codes-and-guidelines/ICESOMAR_Code_English_.pdf
- [9] Scheffler, Hartmut (2015): Ethik in der Marktforschung. Wiesbaden: Springer Fachmedien, p. 15-24.
- [10] SmartResilience: Grant Agreement 01/04/2016

ANNEXES

Annex 1 Review process

Annex 1 Review process

Table 1: Points raised by reviewers and author’s response

Review	Response
Reviewer 1	
Reviewer 2	
Reviewer 3	