RESPONSE

Integrated Solutions for Positive Energy and Resilient Cities

Integrated Solutions for Positive Energy and Resilient Cities

D12.20

Ethical Monitoring and Contingency Plan – V3

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement nº 957751. The document represents the view of the author(s) only and is their sole responsibility: it cannot be considered to reflect the views of the European Commission and/or the European Climate, Infrastructure and Environment Executive Agency (CINEA). The European Commission and the Agency do not accept responsibility for the use that may be made of the information it contains.

Document Control Sheet

Project Title	integRatEd Solutions for POsitive eNergy and resilient CitiEs - RESPONSE
Deliverable	D 12.20 Ethical Monitoring and Contingency Plan – V3
Work package	WP12 Project Management
Task	T12.4 Data and Ethics Management and GDPR Conformation activities
Number of pages	17
Dissemination level	PU
Main authors	Emmanuel Py (UBFC/CID), Pierre Bordais (UBFC/CID)
Contributors	Juuso Virtanen (Turku), Igor Kotsiuba (Isolut), Hadrien Rouchette (Dijon Métropole)

Reviewers

Partner	Name	Contact information
TYS	Matias Salo	matias.salo@tys.fi
EIFER	Monjur Murshed	monjur.murshed@eifer.org

Dissemination level codes

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.

Versioning and Contribution History

Version	Date	Author/Editor	Contributors	Description/Comments
1.0	16/08/2022	Maximilien Lanna Emmanuel Py		Updated version of the deliverable
1.1	28/08/2022		Monjur Murshed	Initial feedback and improvement suggestions
1.2	20/09/2022	Maximilian Lanna Emmanuel Py	WP leaders	Refined version of the deliverable
1.3	07/10/2022		Lamoureux Sini Monjur Murshed Tomi Kultala Catarina Milhazes	Revision and improvement suggestions made by the reviewers and Ethics Board (EtB)
1.4	12/10/2022		Hadrien Rouchette	Description of two Use cases
2.0	23/11/2022	Maximilian Lanna Emmanuel Py	Monjur Murshed	Integration of all feedback and

				preparation of the final version
2.1	15/01/2024	Pierre Bordais Emmanuel Py	Juuso Virtanen Igor Kotsiuba	Update of the relevant European legislation, integration of new usecases
2.2	05/03/2024	Pierre Bordais Emmanuel Py	Ethics board	Integration of the suggestions given by Ethics Board (EtB) and preparation of the final version
2.3	03/04/2024	Pierre Bordais Emmanuel Py	Monjur Murshed	Deliverable sent for review
3.0	16/04/2024	Emmanuel Py	Monjur Murshed, Matias Salo	Integration of reviewers' comments to finalize the deliverable

Table of Contents

Index of Tables

Glossary

Abbreviation	Full form
BTWC	Biological and toxin weapon convention
DPIA	Data Protection Impact Analysis
EC	European Commission
EMCP	Ethical Monitoring and Contingency Plan
ERA	European Research Area
EtB	Ethics Board
EU	European Union
FP7	Seventh Framework Program
GDPR	General Data Protection Regulation
OJ	Official Journal
PIA	Privacy Impact Assessment
QREM	Quality, Risk & Ethics Manager
WHO	World Health Organization
DA	Data Act
DGA	Data Governance Act
DSA	Digital Services Act
DMA	Digital Market Act
AI Act	Artificial Intelligence Act
DORA	Digital Operational Resilience Act
NIS 2	Network and Information Security N° 2 Directive

Executive Summary

This deliverable *D12.20 Ethical Monitoring and Contingency Plan – V3* is the third version of the deliverable related to ethical aspects. The first version (D12.6, submitted on M12) focused on describing Ethics related aspects, including the questions on legal and regulatory compliance in the context of the RESPONSE project. The second version (V2) provided further explanations and guidelines on how to tackle ethical issues. It also provided several example and use cases and, last but not least, new questions that Work Package leaders have to answer when they are trying to identify ethical issues. This version (V3) is an update that mainly provides a synthesis of the ethical and legal issues and some measures taken to deal with them. All changes in the version (V3), compared to the previous version (V2) are highlighted with grey background.

Specifically, this deliverable provides an update of relevant European Union legislation DORA, the AI Act and the NIS 2 Directive (Chapter 2). The Quality, Risk & Ethics Manager (QREM), along with the Ethics Board (EtB) are responsible for the quality and timely delivery of required reports, identification of main areas of possible ethical risks and promotion of appropriate contingency activities. Within the context of RESPONSE project, the ethical risk management policy and two additional relevant use cases in the LHC Turku are described. Then an Ethics Risk Register is introduced to process and monitor ethical issues that could emerge in RESPONSE. Several tools and legal prescriptions (e.g. privacy impact assessment and binding corporate rules) are mentioned that shall be used in order to prevent or dismiss any ethical issues (Chapter 3).

1. Introduction

1.1 Objective

The second version of this deliverable (*D12.19)* has been prepared within the *T12.4 Data and Ethics Management and GDPR Conformation activities* of the RESPONSE project. It covered more issues related to Ethical Monitoring and Contingency Planning (EMCP) and tried to go further in the comprehension of ethics matters in the RESPONSE project.

The objectives of this third version (D12.20) are to :

- Ensure that all legal requirements regarding ethics, personal data protection and data management are understood by the different parties involved (especially Work Package Leaders). It also aims to report new potential ethical issues stemming from the project research activities that haven't been pointed out in the second version of the deliverable.
- Identify and describe some potential use cases related to ethics in the RESPONSE project.
- provide an update of relevant European Union legislation

1.2 Approach

The first version of this document (D12.6) provided an overview of several texts and laws containing ethics elements that should apply to the RESPONSE project. The aim of the second version of the deliverable (D12.19) was to understand if those elements helped to prevent any ethical issues and assess if new one appeared. The goal of the third version of the deliverable (D12.20) is to comprehend the new constraints imposed by the recent digital legislation.

1.3 Relevance to other deliverables

Four versions of the Ethical Monitoring and Contingency Plan will be prepared throughout the RESPONSE project. This D12.20 is the third deliverable, whereas *D12.21 Ethical Monitoring and Contingency Plan – V4* will be prepared in M60

This D12.20 is closely related to the D12.176 Data Management Plan – V4 that will be delivered in M42. It is also linked with D13.1 Ethics Requirement 1, D13.2 POPD Requirement 2, and D12.22 Cyber Data Security and Identity Management Plan – V2, which has been delivered until now. The deliverables provide inputs on how all partners must act in an ethical and responsible manner, especially in activities of data collection and protection involving humans (for example in WP4, WP6, WP7 and 8), use of Informed Consent form in collecting personal data through interviews, surveys, etc. as well as transferring such data within the EU and Non-EU member states.

1.4 Structure of the deliverable

The first part of this deliverable is dedicated to the Ethical Monitoring Plan (Chapter 2). It contains a definition of ethics and a review of the existing literature that can be used in assessing ethics matters. The deliverable presents an overview of several European policies and helps identify aspects that are specifically related to ethics in order to have a comprehensive view of this subject.

Then in Chapter 3, within the context of RESPONSE project, the ethical risk management policy and four related use cases are described. Then an Ethical Risk Register is set, in order to establish 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.

2. Ethical Monitoring Plan

2.1 Ethical Policy

Ethics, in the RESPONSE context, has been explained in deliverable D.12.6. *Ethical Monitoring and Contingency Plan – V1.* As previously stated, it shall be seen as including questions of legal and regulatory compliance as well as a branch of philosophy and shall be seen as an addition to personal data protection matters related in deliverable *D3.2 Data Governance and RESPONSE Integrated and Interconnected City Ecosystem mandating cross-platform collaboration*.

2.1.1 Ethics related legislation overview

Version 1 of the deliverable (D12.6) explained several types of legislation and guidelines related to ethics such as GDPR. Further works on this topic have been realized in the European Union, in order to anticipate the adoption of regulations on the use of artificial intelligence. The Council of Europe, for instance, has adopted guidelines that mention ethical principles[1]. This charter provides a framework of principles that can guide policy makers, legislators and justice professionals when they grapple with the rapid development of AI in national judicial processes. But the ethical principles that are mentioned can also be used in other contexts.

Core principles have been identified and might be useful in the RESPONSE project:

- Principle of respect of fundamental rights: ensuring that the design and implementation of artificial intelligence tools and services are compatible with fundamental rights;
- Principle of non-discrimination: specifically preventing the development or intensification of any discrimination between individuals or groups of individuals;
- Principle of quality and security: with regard to the processing of judicial decisions and data, using certified sources and intangible data with models conceived in a multi-disciplinary manner, in a secure technological environment;
- Principle of transparency, impartiality and fairness: making data processing methods accessible and understandable, authorising external audits;
- Principle "under user control": precluding a prescriptive approach and ensuring that users are informed actors and in control of their choices.

The "European Ethical Charter on the use of artificial intelligence in judicial systems and their environment" is the first European instrument to set out five substantial and methodological principles that apply to the automated processing of judicial decisions and data, based on AI techniques. Developed by the Council of Europe's European Commission for the Efficiency of Justice (CEPEJ), it is aimed at private companies (start-ups active on the market of new technologies applied to legal services - legaltechs), public actors in charge of designing and deploying AI tools and services in this field, public decision-makers in charge of the legislative or regulatory framework, and the development, audit or use of such tools and services, as well as legal professionals.

2.1.2 Data related legislation overview

The second version of this deliverable (D12.19) mainly focused on the adoption of several texts recently adopted at the European level. The European Council's Conclusions of 21-22 October 2021 underlined "the importance of making rapid progress on existing and future initiatives, in particular unlocking the value of data in Europe, notably through a comprehensive regulatory framework that is conducive to innovation and facilitates better data

[1] CEPEJ European Ethical Charter on the use of artificial intelligence (AI) in judicial systems and their environment, Adopted at the 31st plenary meeting of the CEPEJ (Strasbourg, 3-4 December 2018).

portability, fair access to data and ensures interoperability"[2]. In this context, "the Commission puts forward the proposed Data Act with the aim of ensuring fairness in the allocation of value from data among actors in the data economy and to foster access to and use of data"[3]. This version of the deliverable updates the last version by including the DORA, the AI Act and the NIS 2 Directive.

Data Act : The Data Act aims to facilitate consumers' and businesses' access to, and use of, data generated by IoT devices and related services, while prohibiting such data from being used to create competing products or services. Evidently some risks of harm for any project can be anticipated, but by no means all.

Any individual or company who/which has contributed to the generation of IoT data (the "user") is entitled to request access to it from the individual or company (the "data holder") that is entitled or obliged and, regarding non-personal data, able to make the data available. The data shall be made available on fair, reasonable and non-discriminatory terms.

The user and the third party are prohibited from using the data to develop a product that competes with the product from which the data originated. Furthermore, the third party may not onward transfer the data received to another third party, unless this is required to provide the services requested by the user.

The Data Act includes provisions to encourage the development of interoperability standards for data to be reused in different industry sectors to reduce barriers between and within domain-specific data spaces. It also leaves intact the separate rights and obligations under the GDPR that apply to personal data, which must be read in parallel – albeit the Data Act applies to all data, including non-personal data.

Data Governance Act[4]: The Data Governance Act (DGA) has been in force since September 24 2023. It aims to rule the re-use of certain categories of protected data held by public sector body (such as data protected by intellectual property rights, confidentiality, the protection of personal data, ...). Exclusive arrangements regarding data are prohibited and specific conditions for re-use can be imposed by the public sector bodies. Public sector bodies may charge for allowing the re-use od data.

The DGA rules data intermediation services which "aim to establish commercial relationships for the purpose of data sharing between an undetermined number of data subjects and data holders on the one hand and data users on the other, through technical, legal or other means, including for the purpose of exercising the rights of data subjects in relation to personal data (...)". Data intermediation services are provided by a provider that is subject to many obligations to ensure its neutrality.

The DGA also provides "Data Altruism" that allows data subjects to make available voluntary personal data related to them (held by public sector bodies) to be re-use in the general interest.

Digital Services Act[5]: The Digital Services Act (DSA) aims to put into practice the principle that what is illegal offline is illegal online.

It lays down a set of rules to make digital platforms more responsible and to fight against the distribution of illegal or harmful content or illegal products: racist attacks, child pornography, disinformation, sale of drugs or counterfeit goods, etc. This legislation is intended to replace the so-called e-commerce directive of 8 June 2000, which has become outdated.

[2] European Council, European Council meeting (21-22 October 2021) - Conclusion EUCO 17/21, 2021, p. 2.
[3] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on harmonised rules on fair access to and use of data (Data Act), Brussels, 23.2.2022 COM(2022) 68 final 2022/0047 (COD).
[4] REGULATION (EU) 2022/868 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on European data governance and amending Regulation (EU) 2018/1724, 30 May 2022.
[5] REGULATION (EU) 2022/2065 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC (Digital Services Act), 19.10.2022. The regulation shall mainly apply on 17 February 2024 except for some articles that shall apply on 16 November 2022 (article 93§2)

The objectives are multiple: to better protect European Internet users and their fundamental rights (freedom of expression, consumer protection, etc.), to help small businesses in the EU to develop; strengthening democratic control and monitoring of very large platforms; mitigating systemic risks, such as information manipulation or disinformation.

Digital Market Act[6]: The Digital Markets Act (DMA) aims to tackle the anti-competitive practices of the internet giants and correct the imbalances of their dominance in the European digital market. Regulatory tools are put in place upstream to:

- create fair competition between digital players, particularly for the benefit of small and medium-sized enterprises and European start-ups
- stimulate innovation, growth and competitiveness in the digital market
- strengthen the freedom of choise ef European consumers

Artificial Intelligence Act[7] : The Artificial Intelligence Act (AI Act) aims to establish a uniform, technology-neutral definition of AI that could be applied to future AI systems. It proposes that AI systems that can be used in different applications be analyzed and classified according to the risk they pose to users. Different levels of risk will involve more or less regulation. The Parliament's priority is to ensure that AI systems used in the EU are safe, transparent, traceable, non-discriminatory and environmentally friendly. AI systems should be supervised by people rather than automation, to avoid harmful outcomes. On December 9, 2023, Parliament reached a provisional agreement with the Council on the AI Act.

DORA[8] : The Digital Operational Resilience Act (DORA) aims to ensure digital operational resilience[9] within the European Union. It concerns all financial institutions in the European Union. The objectives of the regulation are therefore to unify IT risk management, introduce a procedure for testing IT systems, raise supervisory authorities' awareness of cyber risks and IT-related incidents affecting financial entities. The draft DORA regulation on digital operational resilience was adopted by the European Parliament on November 10, 2022. Its application should be effective within 24 months, i.e. December 2024 or January 2025.

NIS 2[10] : Succeeding the NIS 1 Directive, Network and Information Security n°2 (NIS 2) aims to establish a higher, uniform level of information systems security across the EU. This new directive considerably broadens the scope of the previous regulation, including new sectors such as telecommunications, public administration and social networking platforms and redefining the categories of entities concerned (essential and important entities). Its importance lies in its holistic approach, recognizing that cybersecurity is a shared responsibility, essential to the stability and prosperity of the European digital space. NIS 2 will therefore come into force in France in the second half of 2024, at the latest.

[6] REGULATION (EU) 2022/1925 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on contestable and fair markets in the digital sector and amending Directive (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), 14.09.2022.
[7] REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS
[8] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011
[9] For businesses, resilience is the ability to withstand an event that threatens the continuation of their activity.
[10] DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148.

3. Ethical Risk Management and Contingency Plan

3.1 Ethical Risk Management Policy

The objective of ethical risk management policy is to establish the process to be used to identify, record, manage and monitor ethical risk and the need for contingency planning when an identified risk cannot be completely avoided or mitigated. In relation with guidelines from the European Commission[11], this deliverable focused on several questions that were asked in order to determine if there were ethical problems.

Additional questions can be asked, specifically related to the RESPONSE project:

1. Has there been changes in the way you collect data in the RESPONSE project?
2. Did you feel the need to collect more data than what was originally planned?
3. Did you encounter any difficulties in implementing data protection regulation?
4. Is there a person in charge of data protection in your structure?
5. Is the data safely stored in certified repositories for long term preservation and curation?
6. Do you feel like there might be bias regarding the nature of the data collected? Participants selected to take part in data collection activities show diversity in terms of gender, race, socio-economic background, political stance and disability.
7. What kind of bias: Gender, Race, Political opinion? Were the data collection methods shared with various project partners and the Ethics Board to check for bias, in particular cognitive, unconscious and contextual bias?
8. Were you faced with ethical matters during the realization of project?
9. Do you feel like the Informed Consent Form has been a useful tool?
10. Do you keep trace of every processing of data?
11. Have you been referring to EU texts related to ethics?
    - Which one?
12. Have you identified risks related to data that were not planned at the beginning of the project?
13. Have you been facing security issues with the data collected?
14. Are you concerned by the NIS 2 directive, of 14 December 2022, on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) N° 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148?
    - If yes, how do comply with it?
15. Are you concerned by the directive (EU) 2022/2557, of 14 December 2022, on the resilience of critical entities and repealing Council Directive 2008/114/EC?
    - If yes, how do you comply with it?

The respondants did not notice any relevant evolutions in their behavior that needed to be considered.

3.2 Use cases

Four ethics related use cases (within identification of problems and mitigation strategies) especially within the context of Dijon and Turku lighthouse cities are described in this section. In the next updated deliverable (D12.21), further use cases in context of Turku or Dijon lighthouse cities will be described.

[11] European Commission, Ethics for researchers – Facilitating Research Excellence in FP7, 2013, p. 24.

3.2.1 Ethics use case 1: EcoTouch by OGGA

Eco-Touch technology (provided by the partner OGGA) will be deployed in the PEB2 in Dijon (IE 1.2.3). This tool exploits Artificial Intelligence (AI) for the dynamic management of energy. AI will progressively build the real thermal model of the building and proposes monitoring scenarios without altering the freedom of occupants. It also allows a forecasting of the heating consumption to limit the peak.

Problem: This technology uses knowledge about the presence and absence of the housing occupants (voluntarily shared by the occupants) to finely manage energy consumption. It is crucial to protect the personal data of the occupants.

How to solve: The data must be stored in the building itself, and the storage system shouldn't be accessible from the outside (internet).

3.2.2 Ethics use case 2: CNET bike as a service data collection

CNET bike as a sensor will implement sensors for outside air quality in Dijon on electric bikes and other types of vehicles (mostly buses and tramways). Data gathered by these mobile systems will be sent wireless at specific locations for analysis and contribute to the replicability of mitigation solutions; the holistic impact of energy climate scenarios and test resilience measures (scenarios in Dijon Metropole likely to occur in the coming decades on environment); the effects of each scenario on the territory.

Problem: As the sensor may collect data about its time and location, it may be possible to reconstruct the journey of a given bike.

How to solve: The sensor will only communicate its time, location and serial number to the cloud. It is then possible to install and operate the sensors without declaring the name of the bike in the cloud. There would therefore be anonymisation by compartmentalisation: one environment that will have access to air quality information associated with a serial number; and a second environment where only the users of the sensors will be recorded, without the corresponding locations. As long as the two documents are not combined, anonymity will be respected.

3.2.3 Ethics use case 3: Novel human thermal sensation control

Novel human thermal sensation control (by VTT and Kiona) is implemented in the renovated buildings in Turku's PED area. By using thermal control based on personalized preferences of the resident, the solution aims to improve the indoor thermal comfort of the occupants and the energy efficiency. The Self-sufficient IoT thermostats will be connected to the cloud services via 5G communication hub provided by partner Elisa. VTT's Human Thermal Model calculates an optimal and individual indoor temperature set point value based on the space and the person type living in every room. For this, the algorithm must obtain information about the occupant's physical characteristics, such as age, gender, and body type.

Problem: Information about the occupant's age, gender and physical appearance may reveal personal information about the occupant.

How to solve: VTT will group the apartment specific data into datasets combining at least five apartments, making it impossible to identify single occupants. In addition, the information gathered from the occupant is generalised, so that exact numbers about the person's age or physical dimensions are not collected.

3.2.4 Ethics use case 4: Conflicts between Cybersecurity Measures and Access to Data in Smart City Environments

In the development and deployment of the new technological solutions, services and AI tools, such as Eco-Touch, CNET bike sensors, Novel Human Thermal Sensation Control, and others, ethical considerations regarding data

privacy, consent, transparency, fairness, and accountability must be carefully addressed. These technologies collect and process vast amounts of sensitive data from residents, vehicles, and infrastructure, raising concerns about potential privacy violations, data misuse, and unequal access to benefits and risks.

Problem: The problem lies in the potential conflicts between robust cybersecurity measures and the ethical imperative of ensuring transparent access to data. While stringent security protocols are essential for protecting sensitive information and mitigating cyber risks, overly restrictive measures may hinder data accessibility and transparency, compromising the ethical integrity of smart city initiatives. This creates a delicate balance between safeguarding digital assets and respecting individual rights, necessitating thoughtful consideration and ethical decision-making in the implementation of cybersecurity strategies.

How to solve: Raising awareness about common cyber threats, best practices for data protection, and strategies to mitigate cybersecurity risks is essential for fostering a culture of security and vigilance within the community, which is an ethical imperative. By ensuring that individuals are well-informed about potential risks and how to protect themselves, we uphold the principles of autonomy and empowerment. For this purpose, ISOLUT will provide cybersecurity awareness training and resources to city officials, employees, and residents to educate them about the importance of cybersecurity in smart city initiatives. Through these efforts, we strive to build trust and confidence in smart city initiatives, thereby reinforcing ethical values of transparency, accountability, and respect for individual rights.

3.3 Ethics Risk Register

The Ethics risk register is maintained as a specific project management document. It is stored in the MS Team repository of RESPONSE project and must be continuously updated as soon as ethics related risks become visible. Once a risk is identified by the task leader or the WP leader or even a partner, it shall be submitted to the QREM and EtB who will assess and review it with the respective partners.

Table 1 gives an outline of the ethics risk register of the RESPONSE project, with following information:

- Ethics Risk ID: A unique ID of the ethics risk
- Related WP: Relevancy to the WP
- Ethics Risk Description: Explanation of the identified ethics risk
- Probability: Describes the chances of occurring such risks as low, medium and high
- Impact: Describes the impact of the risks as low, medium and high
- Contingency Plan: Measures to handle the risk in case of its occurrence

Table 1 : Ethics risk register outline of RESPONSE project (stand 15.04.2024)

Ethics Risk ID	Related WP	Ethics Risk Description	Probability (low/medium/high)	Impact (low/medium/high)	Contingency Plan
n° 001	6	Risk of collecting sensible data (according to GDPR) related to health	Medium	Medium	Renewed GDPR Conformity
n° 002	4	Risk of citizen monitoring through data collection	Medium	High	Data minimization and technical solutions related to anonymization
n° 003	3	Multi-scale governance issues related to lack of communication between partners and institutions	Low	High	Grant Agreement Interpretation

n° 004	3	Lack of data from sensors related to data retention from partners	Medium	Medium	Mediation between different partners
n° 005	3	Gender, race, social background, disability, etc related discrimination (based on city data interoperability)	Low	Medium	Ethics by design during data processing
n° 006	5	Risks related to environmental considerations & preservation	Medium	Medium	Reviewing of public contracts
n° 007	3	Risks of conflicts between cybersecurity measures and access to data	Low	High	Reassessment of cybersecurity measures
n° 008	1	Risks of conflicts between national legislations during replication of the project	Low	High	Assess the need for new provisions in the Grant Agreement + Need for negotiations at the European level
n° 009	5	Lack of political and managerial coordination at administrative level to get data to feed the BMC	Medium	High	Dedicated workshop to explain how to fill the BMC
n° 010	5	Lack of clarity of environmental sustainability initiatives	Low	Medium	Improve the connection between LH and FC
n° 011	7	Risk of collecting sensitive data (according to GDPR) related to personal physical details	Medium	Medium	Instead of measuring/collecting data regarding gender, age, height, weight, the tenants are asked to pick a pre-defined fictional person type. Data is stored on VTTs secure servers, not in cloud services. Sensitive data is stored and handled in compliance with GDPR
n° 12	8	Risk of giving an edge to the technical partner in charge of the feasibility study if it followed by a tender process	Medium	Medium	Ensure selection criteria in the tender process will not benefit to the technical partner
n° 013	8	Technical partners may target other priorities and objectives than municipalities	Medium	Low	Try to find compromise to avoid project break up
n° 014	4	The risk of too personal information being published on mentors' social media channels	Medium	Medium	Social media trainings for mentors

4. Conclusion

Ethical monitoring in the RESPONSE project mainly focuses on the risks inherent to the processing of personal data. The aim of the Ethical Monitoring and Contingency Plan is to have a clearer understanding of those risks and to help data processors act in compliance with the renewed legal regime contained in GDPR.

Version 2 of this deliverable (D12.19) focused on legal texts related to ethics and personal data protection law. This Version 3 of the deliverable (D12.20) gives an update on new texts that will soon be applicable: Data Act, Data Governance Act, Digital Market Act, Digital Services Act, AI Act, Digital Operational Resilience Act, Network and Information Security Directive 2.

It also gives a new tool to WP leaders- an ethics risk register that can be completed every time a new question arise, with a risk analysis and suggestions on how to tackle the problem. It also focuses on use cases that shall be useful to every partners. The next versions of this deliverable will be D12.21 (M60), where further updates and use cases will be presented.

Bibliography

- Horizon 2020 Programme: Guidance on How to complete your ethics self-assessment, h2020_hi_ethics-self-assess_en.pdf (europa.eu)

- "H2020 Programme Guidelines on FAIR Data Management in Horizon 2020", h2020-hi-oa-data-mgt_en.pdf (europa.eu)

- H2020 Programme Guidelines to the Rules on Open Access to Scientific Publications and Open Access to Research Data in Horizon 2020, h2020-hi-oa-pilot-guide_en.pdf (europa.eu)

- EDPB, Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) Version 2.1 12 November 2019, 28 p.

RESPONSE

Integrated Solutions for Positive Energy and Resilient Cities

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement nº 957751. The document represents the view of the author(s) only and is their sole responsibility: it cannot be considered to reflect the views of the European Commission and/or the European Climate, Infrastructure and Environment Executive Agency (CINEA). The European Commission and the Agency do not accept responsibility for the use that may be made of the information it contains.