COMPAIR

DELIVERABLE

D7.2 Legal Requirements and Guide to Legal Compliance for Data-Driven Decision Making

Project Acronym:	**COMPAIR**	
Project title:	Community Observation Measurement & Participation in AIR Science	
Grant Agreement No.	101036563	
Website:	www.wecompair.eu	
Version:	1.0	
Date:	31 October 2024	
Responsible Partner:	UAEG	
Contributing Partners:	DV	
Reviewers:	Internal: DV (AIV), ISP External: Andrew Stott, Joep Crompvoets	
Dissemination Level:	Public	X
	Confidential, only for members of the consortium (including the Commission Services)	

This project has received financial support from the European Union's Horizon 2020 Programme under grant agreement no. 101036563

Revision History

Version	Date	Author	Organization	Description
0.1	1/3/2023	Vasiliki Diamantopoulou	UAEG	Initial structure
0.2	12/3/2023	Vasiliki Diamantopoulou, Athanasia Orfanou	UAEG	Initial content
0.3	13/03/2023	Jiri Bouchal, Martine Delannoy	ISP DV	Initial review, corrections and further development
0.4	8/01/2024	Vlatko Vilovic Sylvain Renault Sakis Dalianis Christos Karelis	INT3 HHI ATC UAEG	Input added from pilot partners
0.5	14/10/2024	Jiri Bouchal, Martine	DV (AIV), ISP	Internal review
0.6	15/10/2024	Vasiliki Diamantopoulou	UAEG	Input added
0.7	22/10/2024	Athanasios Dalianis, Marina Klitsi	ATC	Input added
0.6	22/10/2024	Vasiliki Diamantopoulou	UAEG	Final draft
0.7	24/10/2024	Andrew Stott Joep Crompvoets	external	External review
1.0	31/10/2024	Vasiliki Diamantopoulou	UAEG	Final version

Table of Contents

List of Abbreviations

Abbreviation	Definition
CO2	Carbon Dioxide
CS	Citizen Science
DAEM	Dimos Athinaion Epicheirisi Michanografisis
DEV-D	Dynamic Exposure Visualisation Dashboard
DEVA	Dynamic Exposure Visualisation Application
DoD	Department of Defense
EAP	Energy Agency of Plovdiv Association
GDPR	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/ (General Data Protection Regulation)
IEEE	Institute of Electrical and Electronics Engineers
INT3	Inter 3 Gmbh Institut fur Ressourcenmanagement
NIST	National Institute of Standards and Technology
PMD	Policy Monitoring Dashboard
SDA	Assotsiatsia za Razvitie na Sofia
SES groups	Socio Economic Status groups
VMM	Vlaamse Milieumaatschappij

Executive Summary

This deliverable provides information on what kind of personal data was collected and processed within the COMPAIR project and which steps have been taken to ensure their secure and lawful processing. It describes the technical and organisational measures for safeguarding the rights and freedoms of the data subjects participating in research, specifically under the context of (automated) decision-making tools and processes and describes the security measures used to protect the personal data, and the six GDPR principles that are satisfied within the COMPAIR research project.

The provision of the above mentioned information is given as a guide for future CS projects and initiatives. The deliverable describes the legal requirements they should take into consideration in order to protect the personal data they process. These requirements can also help relevant policy makers in their attempt to reach legal compliance for data-driven decision-making. This deliverable concentrates on the following points:

- Organisational Measures: the organisational measures institutionalised in the host organisations DAEM for the Athens use case, INT3 for the Berlin use case, VMM for the Flanders use case, SDA for the Sofia use case, and EAP for the Plovdiv use case.
- Technical Measures: the technical measures applied for processing personal data and the security measures implemented to prevent unauthorised access to personal data. This document also describes security techniques that were implemented in order to fortify project's data.
- Terms and Conditions for the use of Apps and Dashboards: description of the Privacy Policies that applied to allow partners to use the COMPAIR Apps and Dashboards in order to collect and process the necessary data.

The thorough examination of the GDPR has equipped the project's partners with a comprehensive understanding of the legal landscape surrounding data protection and privacy. By identifying key compliance requirements, a solid foundation can be laid for ensuring that all projects' activities align with the standards set forth by the legislation. This proactive approach underscores a project's (COMPAIR included) commitment to safeguarding personal data and upholding the rights of individuals. Following this extensive analysis, this project's tools were successfully deployed with a strong emphasis on compliance. Each tool was designed and implemented with the necessary safeguards to ensure adherence to the fundamental GDPR principles, including data minimization, purpose limitation, and transparency.

By integrating compliance measures into the core functionality of a project's tools, one can not only mitigate potential risks but also foster trust with the participants.

Finally, this deliverable highlights the approaches that were used during the pilot campaigns of the project, focusing on the handling of vulnerable groups. These recommendations are the outcome of lessons learned during the execution of the pilots and can and should be considered as guidelines for future CS projects and initiatives.

1. Introduction

In the COMPAIR project, personal data have been collected, stored, and processed in the COMPAIR platform, that comprises of four discrete tools, namely, Policy Monitoring Dashboard (PMD), CO2 Simulation Dashboard, Dynamic Exposure Visualisation Dashboard (DEV-D) and Dynamic Exposure Visualisation Application (DEVA), during the validation and demonstration of the COMPAIR platform in the Athens, Berlin, Flanders, Sofia, Plovdiv pilots. The data processing took place online with automated means in the COMPAIR Cloud or offline manually by COMPAIR researchers to validate and demonstrate the provided solution.

DAEM coordinated Athens use case, INT3 the Berlin use case, VMM the Flanders use case, SDA the Sofia use case and EAP the Plovdiv use case. Each partner stored and processed its data within its own premises. Any data being shared within COMPAIR was stored and processed on the COMPAIR Cloud hosted by DV. Some of the tools / products being used for the project depend on cloud services provided by the respective partner that may store and process tool-specific data.

For any of these data-sharing scenarios, COMPAIR achieved to minimise storage and processing of personal data, to establish effective protection mechanisms, and to follow procedures to comply with the rules of the General Data Protection Regulation. For operationalising personal data protection, COMPAIR followed the principles and recommendations specified in the European Commission's Ethics and Data Protection awareness-raising document (European Commision, 2018).

1.1 Purpose of this Deliverable

The aim of the deliverable and the emerging guidelines is to provide an easy to understand guide for Citizens Science (CS) projects and policy makers on the legal necessities for CS initiatives and CS data use. The target audience of this document is policy makers and future CS initiatives that will exploit COMPAIR findings for the appropriate use of the data they will process.

1.2 Structure of this Deliverable

The rest of the deliverable is structured as follows: Section 2, entitled "COMPAIR and General Data Protection Regulation" highlights the critical relevance of GDPR compliance. Within this chapter, we elaborate on the six principles of GDPR that underpin a project's approach to reach compliance. Chapter 3 focuses on the specific security measures than can be implemented to safeguard data, with Section 3.1 analysing the implications of legal requirements on decision making process, Section 3.2 detailing the security and privacy measures that should be implemented to fortify personal data within a research project; Section 3.3 outlining the organisational measures that should be established to ensure data protection; and Section 3.4 discussing the data protection measures that can be applied at

the tool level. Chapter 4 addresses the handling of vulnerable groups, emphasising the commitment to protecting SES groups. Finally, Chapter 5 presents the conclusions finalising the document.

2. COMPAIR and General Data Protection Regulation

Regulation (EU) 2016/679 on the protection of natural persons concerning the processing of personal data and on the free movement of such data (the General Data Protection Regulation, or the GDPR) lays down the principles, rules and procedures to be followed by any actors involved in processing of personal data related to individual natural persons residing in the EU, or any personal data processing by actors established in one or more EU Member States. According to the GDPR, the use or consultation of personal data is considered “data processing”. This means that data used for decision-making will fall within the GDPR’s scope of application, to the extent they are personal data (Article 4(2) GDPR). This requirement applies whether the processing is conducted manually or by using autonomous systems (e.g. supported by AI algorithms) (Article 2(1) GDPR).

A research project (the Consortium) is considered the data controller, since it processes personal data it collects during the pilot rounds. GDPR outlines six data protection principles that organisations shall abide by when collecting (Diamantopoulou et al., 2022), processing and storing individuals’ personal data:

1. **Lawfulness, fairness and transparency:** personal data must be processed in a lawful and transparent manner, ensuring fairness towards the individuals whose personal data is being processed.
2. **Purpose limitation:** there must be specific purposes for processing the data and the company/organisation must indicate those purposes to individuals when collecting their personal data. A company/organisation cannot simply collect personal data for undefined purposes and further use the personal data for other purposes that are not compatible with the original purpose, except for under certain narrow circumstances.
3. **Data minimisation:** The company/organisation may collect and process only personal data to the extent that is necessary to fulfil that purpose.
4. **Accuracy:** The company/organisation must ensure personal data is accurate and up-to-date, having regard to the purposes for which it is processed, and rectify the data where it is not.
5. **Storage limitation:** the company/organisation must ensure that personal data is stored for no longer than necessary for the purposes for which it was collected.
6. **Integrity and confidentiality:** the company/organisation must install appropriate technical and organisational safeguards that ensure the security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technology.

In the next paragraphs these principles are analysed with respect to how they have been tackled within COMPAIR activities, as follows:

1. Lawfulness, fairness and transparency

COMPAIR is a research project and its main focus is to bolster citizens' capacity to monitor, understand, and change their environmental impact, both at a behavioural and policy level. The personal data was collected during the pilot campaigns that took place in 5 different cities in Europe. For the communication, and the interaction of the pilot partners with the volunteers in each pilot city, each data subject was provided with its **consent form** (Article 6(a)) (the templates of the consent forms that were used can be found in Annex) in order for COMPAIR to process its data. By reading this form, data subjects can be **informed about** the scope of the project and the research aspects that the collection of their data would contribute to, and about the project partners and contact details. Additionally, this consent form contained the **privacy policy of each tool**. Through this text, the volunteers were informed about the personal data being processed, the time of storage of the data, their rights, as well as the security measures that have been put in place.

2. Purpose limitation

Another GDPR-related principle is purpose limitation, the principle under which personal data shall be processed for **specified, explicit and legitimate purposes** and not further processed in a manner that is incompatible with those purposes. This principle is enshrined under Art. 5(1)(b) of the GDPR and requires personal data to be collected and processed for the original purpose of collection of the data, or, at least, so long as it is not incompatible with the original purpose.

Whatever the main focus of a project or initiative may be (the main focus of the COMPAIR project is to bolster citizens' capacity to monitor, understand, and change their environmental impact, both at a behavioural and policy level). Under this scope, environmental and personal data is collected and processed, using the tools / dashboards that have been developed during the project. The collected data **cannot be used for any other scope** during the project and after this data is not necessary any more for the needs of the research activities of the project, the corresponding partners have to **proceed to its secure deletion**, following specific instructions (presented in Section 3.2.4 of this deliverable).

3. Data minimisation

The data minimisation principle means that **only** this **data** is used or consulted for decision-making that is **necessary**. Processing of any excess data is unnecessary, thereby creating unnecessary risks, which may vary from hacking to unreliable inferences resulting in incorrect, wrongful, and potentially dangerous decisions. The European Commission also notes that “generating and processing less data limits the security risks. Therefore the compliance with data minimisation measures also provides for security safeguards” (European Commission, 2020). Adhering to the data minimisation principle can therefore be recommended as a good practice for handling non-personal data as well.

An initiative aiming at lawful, fair, and transparent data processing should **design its processes** in order **to involve only the necessary and proportionate data** to deliver its services to its end-users / participants.

The initiative should minimise the amount of personal data being collected. **Only the data** should be collected that is **necessary to meet the research objectives** for validation and demonstration of the solution, or any monitoring or simulation tools it may provide / contain.

The initiative should finally **minimise the extent** to which personal data may be accessed, further **processed**, and **shared**, the **purposes** for which they are used, **and the period for which they are kept**.

4. Accuracy

Personal data must be accurate and where necessary kept up-to-date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay. With this principle, the GDPR recognises that issues with data accuracy or completeness may lead to unfair and non-transparent handling of personal data, and impact on data subjects' right to privacy.

Data subjects should be given the ability to **rectify their data** via provisioning of a suitable mechanism (for instance by using an email address that can be provided through the Consent Form (see Annex)) so that they can review or correct it if they wish to review or rectify any information.

5. Storage limitation

Storage limitation principle imposes that data controllers are transparent about the time period they intend to store data for the specified purposes. Storage limitation is a GDPR requirement not to store data for longer than necessary for its processing.

Most EU projects deliver their results **at the end of the project**, at the final review. After this period, the collected data is not necessary anymore, since all the results of the processing would have been included in the corresponding deliverables of the project and in the scientific research works that have already been published, or they will be published soon. To this end, all relevant stakeholders (e.g. policy makers, partners of CS projects) that process personal data (of the participants to the pilots) can follow specific instructions (presented in Section 3.1.2.1 of this deliverable) in order to **securely erase this data**.

6. Integrity and confidentiality

Organisations and initiatives handling the data must use appropriate technical and organisational measures that ensure an appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. This principle is thoroughly analysed in Section 3 of this document.

3. Measures to safeguard data

The main goal of the COMPAIR project is to provide a well-rounded view of air pollution and related challenges, such as traffic, waste management, energy use, etc. This is achieved by designing advanced monitoring and simulation tools in order to aggregate data from multiple sources and to present them in such a way that would be of value for the research community.
Besides the environmental data, the tools and dashboards that were designed for COMPAIR project collected also personal data from volunteers that participated in the open rounds that took place in various cities of Europe (i.e. Athens, Berlin, Flanders, Plovdiv, and Sofia). During the initial iterations for the design phase of these tools, **one of the main concerns** was the application of **security- and privacy-by-design** principles, to protect both the business and the personal data that were used in the project, safeguarding the rights and freedoms of the data subjects that participated in the research.

COMPAIR, as an innovation project designed to bolster citizens' capacity to monitor, understand, and change their environmental impact, both at a behavioural and policy level, makes new information useful for research purposes, (automated) policy making. Article 22 of the GDPR is applicable to projects (among others) dealing with Automated Decision Making.

3.1. The implications of legal requirements on decision making

Data-driven decision-making processes have become integral to modern organisations, enabling them to leverage insights derived from data analytics to inform strategic initiatives and operational improvements. However, the effectiveness of these processes can be significantly influenced by legal requirements surrounding data collection, usage, and protection. Regulations such as the General Data Protection Regulation (GDPR)) impose strict guidelines on how personal data is gathered, stored, and analysed, necessitating that organisations implement robust compliance frameworks. Failure to adhere to these legal standards not only risks hefty fines and legal repercussions but can also undermine the integrity of the data being utilised for decision-making, leading to potentially flawed conclusions.

Moreover, the impact of legal requirements extends beyond compliance; it shapes the ethical considerations of data use within organisations. As businesses navigate the complexities of data governance, they must balance the pursuit of insights with the imperative to respect individual privacy rights. This dynamic often leads to the adoption of more transparent and responsible data practices, which can enhance stakeholder trust and foster a positive organisational reputation. By integrating legal compliance into their data-driven decision-making processes, initiatives can ensure that their strategies are not only effective but also ethically sound, positioning themselves for sustainable growth in an increasingly data-centric landscape.

Article 22 of the GDPR is applicable to projects (among others) dealing with Automated Decision Making. More specifically, per the Regulation, “the data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her”, unless if “the decision is based on the data subject's explicit consent”. In projects and initiatives like COMPAIR, the **consent** of the data subjects should be **the lawful basis** for the processing of their personal data.

3.2. Security and Privacy Measures

Ensuring the security of personal information is a critical responsibility for research projects, particularly in the context of GDPR compliance. This chapter explores the essential security measures that our (and future) research project has implemented and must continuously evaluate to protect the data it handles. By adhering to the **principles of security-by-design**, a project will be more successful in integrating robust security mechanisms and procedures throughout the data lifecycle, from collection and processing to storage, and erasure. This proactive approach not only mitigates risks but also fosters trust among participants and stakeholders. Additionally, we will examine key topics and best practices, like **privacy-by-design** that can be employed to safeguard the personal data that a project collects and processes, ensuring that the project remains compliant with GDPR requirements while upholding the highest standards of data protection.

3.2.1 Security- and Privacy-by-design

A project aiming to implement a "security by design" framework, recognizes that security must be an integral component of the system development life cycle rather than an afterthought (Bygrave, 2022; Ebad, 2022). By prioritising security from the very outset, a project proactively identifies and mitigates potential vulnerabilities while ensuring that robust protection measures are embedded at every stage of design and development. This approach encompasses a thorough analysis of the system’s architecture and actions to be taken, aligning them with industry standards and best practices. The goal should be to create a secure environment that not only protects personal data and user security but also fosters confidence among stakeholders, ultimately leading to a resilient and trustworthy solution in an increasingly complex digital landscape.

Specifically, throughout the project, an **internal discussion / consultation** can be conducted with the research team to ensure that data is collected on **a “need to know” basis**, i.e. the data is required for a specific purpose that is relevant and limited to the project's objectives. After this process, the aforementioned tools and dashboards can be designed and developed for the needs of the project, taking into account privacy by design principles (Articles 5 and 25 of the Regulation (EU) 2016/679 (General Data Protection Regulation); Chapter IV of 'Ethics and data protection', European Commission). The principle of data minimization should be addressed, by **only including data** that is **necessary** and **proportionate** to achieve the project's research objectives. Additionally, the

storage of the data is advised to be conducted using in-house storage with appropriate security measures.

To ensure compliance with the privacy-by-design principles, any research project developing tools that process personal data, must **embed privacy considerations** at every stage of its lifecycle. The project should adopt data minimization, collecting only the data strictly necessary for its purpose, and ensure that the identity of the data subjects cannot be revealed. Consent mechanisms must be made transparent, with users informed of how their data is being used and given control over its collection, retention, and deletion. Finally, participants must be informed of the rights they can exercise, i.e. right to access, review, and rectify the data, right to erasure, right to object or restriction of processing, right to data portability.

3.2.2 Encryption

Digital data[1] is diverse in type and purpose. However, all data can be generally classified into three different states:

- data at rest,
- data in transit, and
- data in use.

These states represent where the data is in the system and how it's being used at the given moment. Different encryptions schemes can be applied, according to the different data types:

Encryption at Rest

Encryption at rest[2] refers to the encryption of data while it is stored in a device or a storage system. Data at rest is defined as not being actively used, such as moving between devices or networks and not interacting with third parties. This includes hard drives, USB drives, and cloud storage. The purpose of encryption at rest is to protect data from unauthorised access in case of theft, loss, or physical damage to the storage device.

While data is generally less vulnerable at rest than in transit, often, hackers find the data at rest more valuable than data in transit[3] because it often has a higher level of sensitive information–making this data state crucial for encryption. One thing to note: many data breaches happen due to a lost USB drive or laptop – just because data is at rest doesn't mean it won't move.

Encryption at rest works by converting plain text data into ciphertext using an encryption algorithm and a secret key. The encrypted data can only be accessed using the secret key.

---

[1] https://jatheon.com/blog/data-at-rest-data-in-motion-data-in-use/
[2] https://www.basusa.com/blog/data-encryption-at-rest-and-in-transit
[3] https://datalocker.com/technology/encryption/encryption-at-rest-vs-in-transit-effectively-encrypt-identifiable-information/

The key is typically stored separately from the encrypted data to prevent unauthorised access. Encryption at rest can be implemented at various levels, including the file system, the database, and the application layer.

Encryption in Transit

Encryption in transit is when the encrypted data is active, moving between devices and networks such as the internet, within a company, or being uploaded in the cloud, in other words it refers to the encryption of data while it is being transmitted from one device to another over a network. This includes data transmitted over the internet, local area networks (LANs), and wide area networks (WANs). The purpose of encryption in transit is to protect data from interception, eavesdropping, and tampering during transmission.

Encryption in transit works by encrypting the data using an encryption algorithm and a secret key before transmitting it over the network. The encrypted data can only be decrypted using the secret key at the receiving end. The key is typically exchanged using a secure key exchange protocol such as Secure Sockets Layer (SSL) or its successor, the Transport Layer Security (TLS).

For the purposes of a research project working with personal data to be used for decision-making, encryption should be used, at a level proportionate to the data being processed.

Encryption in use

Encryption in use protects data in memory from compromise or data exfiltration by encrypting it while it is being processed. When data is in use, the central processing unit of the hardware is doing something to the data, such as coding, viewing, or playing a file. Anytime a program is being updated, erased, viewed, or generated, it is considered in use. This is a difficult stage for encryption since the implementation could potentially crash or damage the application accessing the data but is also critical to protect the information in this state as well. Although this is a tricky state to encrypt, unencrypted data in use creates a huge risk factor for data breaches.

Finally, modern enterprise HDDs and SSDs provide an option to have hardware encryption using an external key supplied at each power-up. If the drive is stolen, the encryption protects the data.

3.2.3 Data documentation

During a project, establishing a **clear and systematic process for documenting the storage locations of personal data** is essential. This procedural framework serves multiple purposes, primarily ensuring that all data is tracked meticulously throughout its lifecycle. By maintaining comprehensive records of where personal data is stored, projects and initiatives can streamline the management of this data and enhance compliance with data protection regulations, such as GDPR.

Furthermore, having a documented process allows for efficient identification and retrieval of personal data when the purpose for its processing has been fulfilled (in our case, this is at the end of the project). This capability is vital for facilitating timely and secure deletion, thereby reducing the risks associated with prolonged data retention. In addition, it supports accountability and transparency within the organisation, demonstrating a commitment to protecting individual privacy rights.

Moreover, a well-defined documentation process can improve communication among project stakeholders, fostering a culture of data responsibility and awareness. By prioritising data management from the outset, organisations not only safeguard sensitive information but also build trust with clients and users, ultimately contributing to a more ethical and compliant operational environment.

3.2.4 Data erasure

With data usage expected to reach 221 zettabytes by 2026 and breach costs averaging $4.88 million, minimise attack surface by securely erasing data and devices is more important than ever[4].
The modern storage environment is rapidly evolving. Data may pass through multiple organisations, systems, and storage media in its lifetime. The pervasive nature of data propagation is only increasing as the Internet and data storage systems move towards a distributed cloud-based architecture (NIST, 2014). As a result, more parties than ever are responsible for effectively sanitising media and the potential is substantial for sensitive data to be collected and retained on the media. This responsibility is not limited to those organisations that are the originators or final resting places of sensitive data, but also intermediaries who transiently store or process the information along the way. The efficient and effective management of information from inception through disposition is the responsibility of all those who have handled the data.
To effectively erase previously stored data, the simplest techniques overwrite hard disk drive storage areas with the same data everywhere - often using a pattern of all zeros.
Modern standards nowadays take overwriting a step further with prescribed random overwriting methods. At a minimum, such applications will prevent the data from being retrieved through standard data recovery methods. Choosing the right data erasure standard is crucial for securing end-of-life data and maintaining compliance with applicable data privacy laws.
The most commonly used standards and methods for data erasure are the following:

- **The DoD 5220.22-M method:** The DoD 5220.22-M method for data erasure first appeared in the early days of the data sanitization industry. The process required three secure overwriting passes and verification at the end of the final pass. Verifications have spun, like the DoD long wipe, with 7 passes, and even 35 passes (Gutmann's method), although many sources argue that with today's technology, one pass is enough.
- **NIST 800-88 Guidelines for Media Sanitization:** NIST Special Publication 800-88 has become the go-to data erasure standard, at least in the United States. Originally

[4] https://www.blancco.com/resources/dod-nist-or-ieee-modern-data-sanitization-standards/

issued in 2006 and revised in December 2014, this publication addresses flash-based storage and mobile devices, which weren't considered under the DoD process. It outlines the preferred methodologies for data sanitization for hard drives, peripherals, magnetic and optical storage and other storage media. NIST describes three methods that can help ensure that data is not unintentionally accessed, namely, NIST Clear, NIST Purge and NIST Destroy.

- **IEEE Standard for Sanitizing Storage:** IEEE 2883 adopts a similar framework with categories of Clear, Purge, and Destruct. However, IEEE standards are often quicker to execute and incorporate newer data destruction capabilities introduced since 2015, such as restoring depopulated storage elements, resetting write pointers, and clearing NVMe buffers. A notable distinction between the two is IEEE's deprecation of shredding and pulverising as methods of sanitization. This change reflects the increasing density of information on modern storage devices and the consequent risk of data remnants on fragments.
- **Physical destruction:** If the drives are no longer required, another method to achieve data sanitization is physical destruction through melting, crushing, incineration or shredding. Physical destruction is not ideal if someone wants to reuse their drives, as they'll be completely destroyed, but even this method isn't necessarily absolute. If any disk pieces remain large enough after destruction (especially on SSDs), they can still contain recoverable information.
- **Sanitization Methods in Summary[5]:**

***Table 1**: Sanitization methods*

Method	Description
Clear	Use software or hardware products to overwrite user-addressable storage space on the media with non-sensitive data, using the standard read and write commands for the device. This process may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table) but also should include all user-addressable locations. The security goal of the overwriting process is to replace target data with non-sensitive data. The media type and size may also influence whether overwriting is a suitable sanitization method. For example, flash memory-based storage devices may contain spare cells and perform wear levelling, making it infeasible for a user to sanitise all previous data using this approach.
Purge	Purging includes overwrite, block erase, and Cryptographic Erase, through the use of dedicated, standardised device sanitise commands that apply media-specific techniques to

5 https://docs.opswat.com/mdkiosk/v4.7.1/knowledge-base/what-is-the-difference-between-the-format--1-pass--3-pass--and-7

	bypass the abstraction inherent in typical read and write commands. Destructive techniques also render the device Purged when effectively applied to the appropriate media type, including incineration, shredding, disintegrating, degaussing, and pulverising. The common benefit across all these approaches is assurance that the data is infeasible to recover using state of the art laboratory techniques. However, Bending, Cutting, and the use of some emergency procedures (such as using a firearm to shoot a hole through a storage device) may only damage the media as portions of the media may remain undamaged and therefore accessible using advanced laboratory techniques. Degaussing renders a Legacy Magnetic Device Purged when the strength of the degausser is carefully matched to the media coercivity.
Destroy	There are many different types, techniques, and procedures for media Destruction. While some techniques may render the Target Data infeasible to retrieve through the device interface and unable to be used for subsequent storage of data, the device is not considered Destroyed unless Target Data retrieval is infeasible using state of the art laboratory techniques. ● *Disintegrate, Pulverize, Melt, and Incinerate*. These sanitization methods are designed to completely Destroy the media. They are typically carried out at an outsourced metal Destruction or licensed incineration facility with the specific capabilities to perform these activities effectively, securely, and safely. ● *Shred*. Shredders can be used to Destroy flexible media such as diskettes once the media are physically removed from their outer containers. The shred size of the refuse should be small enough that there is reasonable assurance in proportion to the data confidentiality that the data cannot be reconstructed. The application of Destructive techniques may be the only option when the media fails and other Clear or Purge techniques cannot be effectively applied to the media, or when the verification of Clear or Purge methods fails (for known or unknown reasons).

- **Verification / Certification of Erasure:** The goal of sanitisation verification is to ensure that the target data was effectively sanitised. When supported by the device interface (such as an ATA or SCSI storage device or solid state drive), the highest level of assurance of effective sanitisation (outside of a laboratory) is typically achieved by a full reading of all accessible areas to verify that the expected sanitised value is in all addressable locations. A full verification should be performed if time

and external factors permit. Following sanitization, a certificate of media disposition should be completed for each piece of electronic media that has been sanitised.

Guidelines for secure deletion of data

A project / initiative can collect various types of data during the pilot rounds. What has been determined and what the Privacy Policy of the project should mention is that the collected data have to be securely deleted by the end of the project. In order to achieve secure erasing of data, all relevant members / partners / stakeholders have to comply with this obligation. Below, we summarise the instructions that should be followed by similar projects (but in general as well) for secure erasing of data.

- **For data stored in HDDs / SSDs:**
  Use any software complying with the DoD 5220.22-M data sanitization method (also called the *DoD 3-pass method* or *DoD short wipe*). In short, the user should format (or quick format) the HDD/SSD), overwrite all addressable locations with binary zeroes, overwrite all addressable locations with binary ones, and overwrite all addressable locations with a random bit pattern. Nowadays, HDD / SSD manufacturers provide software capable of performing secure erase, for instance via including commands that allow the original randomly-generated internal-only key to be deleted and replaced, making the old contents essentially random bits. However, an easy/free solution is the following:
    - In a Windows machine plug the HDD / SSD
    - Quick Format the disk (Right Click → Format)
    - Run command (in a cmd prompt) “cipher /w:M:” where M is the drive letter
- **For data stored in Physical Media (CDs, DVDs etc.):**
  Physical destruction of the media should be used. There are specific devices available to this aim, however, an easy/free solution is to use a hammer or drill. Just make sure to destroy the whole surface area of the media (a drill hole is not enough).
- **Data stored in Mobile Devices:**
  There are applications available offering secure deletion of data. However, an easy/free solution is the following:
    - If the data is stored in a removable SD card, remove the card from the device, plug it into a Windows machine, and use the procedure used for HDDs / SSDs.
    - For data stored internally in the device, reset the device to the factory settings, search for remaining traces of the files and erase them, then reset to the factory setting again. This three-step process is not a guaranteed fix, but a good option.
- **For Hardcopies:**
  A shredder, typically found nowadays, is enough to destroy the data.
- **For data stored in the Cloud:**
  A cloud storage provider that complies with NIST or equivalent guidelines (offering secure deletion) should be used. If not, there is no guarantee that the data will be securely erased. Still, the provided (permanent) delete procedure should be used.

Furthermore, if this is an option, companies provide secure deletion of data as a service, where a certificate of erasure is offered. However, this is an overkill for the type of data stored in the COMPAIR project, since no sensitive personal data was stored.

3.3. Organisational Measures

A project / initiative can implement various organisational measures in order to safeguard the rights and freedoms of the data subjects being research participants and contributors/volunteers. These measures (per the COMPAIR approach) include appointing a designated contact person from the consortium as the Privacy and Ethics manager, creating specific privacy policies for each tool, and the gathering of consent forms from each pilot.

3.3.1. Designated Contact Person

As described in the deliverable D1.7 “Data Management”, each partner can appoint a Data Protection Officer in order to supervise the activities in the project related to the processing of data. Additionally, one person from the UAEG, (in our case this person was Vasiliki Diamantopoulou), can be given the role of the Privacy and Ethics manager who can supervise the documents and actions related to the processing of the personal data that the project collects and exploits for decision-making.

3.3.2. Privacy Policies

A general privacy policy should be published (Brunottte et al., 2022) that presents all the data that the project collects and processes by the visitors of its website (for our project: https://www.wecompair.eu/). It also informs the data subjects of how the collected information is being used (our privacy policy can be found in the following url: https://www.wecompair.eu/terms-and-conditions).

Also, when the tools / dashboards are developed and are ready to be used by the pilots, a specific privacy policy for each tool / dashboard should be published. The need for this action is that each tool most probably is distinct and processes different types of personal data (within COMPAIR, a dedicated privacy policy was developed for the Dynamic Exposure Visualisation Application (DEVA) and the Dynamic Exposure Visualisation Dashboard (DEV-D) and can be found in the link: https://monitoring.wecompair.eu/dashboards/dev-d/DEVD-privacy-policy and a dedicated privacy policy was developed for the CO2 Calculator and can be found in the following link:https://monitoring.wecompair.eu/dashboards/carbon-footprint/CO2-privacy-policy).

Finally, if there are any tools that don’t process any personal data (like the Policy Monitoring Dashboard (PMD) of COMPAIR, which according to the information in Table 2 of this document, it doesn’t process any personal data), they need not have a specific privacy policy. However, all tools can be linked to the general ‘Terms and Conditions’ of the project.

3.3.3. Consent Forms

Valuable lessons have also been learned for designing consent form(s). As it has been described in deliverable D5.6 “Public Round Report”, during the project, 5 different pilot scenarios were conducted in order for the partners to explore the activities of each tool, running various use cases. These rounds resulted in valuable lessons learned that are presented in detail in D5.6.

Specifically, the pilot projects were conducted in five different cities, namely, Athens, Berlin, Flanders, Plovdiv and Sofia. What should be highlighted is that these pilots used different tools, and under different use cases they explored the capabilities of each tool in order to provide useful results for the project, aiming to support decision-making. For this reason, five different and specific consent forms (Luehnen et al., 2018) (available in the Annex of this document) were developed and used by each responsible pilot partner when they were interacting with the participants / volunteers.

Therefore, it is advised for future initiatives and CS to design, distribute, and collect **consent forms specific** per test case and / or tool.

3.4. Data Protection Measures at Tool-Level

During a project’s life cycle, different tools can be developed and deployed. For instance, in the COMPAIR project, 4 tools and apps were developed, aiming at the aggregation of data from multiple sources in order to provide a clear view of air pollution, traffic, waste management, energy use, etc. These tools, namely, Policy Monitoring Dashboard (PMD), CO2 Simulation Dashboard, Dynamic Exposure Visualisation Dashboard (DEV-D), and Dynamic Exposure Visualisation App (DEVA), which are specified in detail in the deliverable D4.5 Digital Twin CS data integration and prototype 3.

Various security and privacy measures must be put in place, both technical and organisational ones, in order to safeguard the data that tools are processing. Table 1-Table 3, presents the measures that have been applied in COMPAIR. As can be seen in these tables, each tool can implement **specific protection measures**, which are **proportional** to the level of criticality of the data that they process.

All tools function as standalone components and do not require user registration (for their use). However, users can access information about the project’s offerings, including general information and dashboards, via the landing page (for COMPAIR: https://monitoring.wecompair.eu). A registration process may be required only for implementing specific dashboards. During registration, personal information (name, email, password) can be collected and securely stored in the project’s database(s) (in the case of COMPAIR these were hosted by the Project Coordinator). All communication between publicly available APIs should be **secured via HTTPS** and managed by an API Gateway that controls data flow. In addition to HTTPS, platforms should use user- and / or role-based **authentication** (for example, for COMPAIR this was realised via use of the JWT framework), ensuring that only registered users with appropriate roles have access. Users and roles can

also be defined at the database level, granting different privileges to users based on their roles.

Passwords must be **encrypted**, and all data handling must comply with GDPR regulations. However, in today's security landscape, merely encrypting passwords is no longer sufficient to protect sensitive data from unauthorised access. To enhance security, it is essential to employ **robust practices such as salting and hashing passwords** using algorithms that are resistant to brute-force attacks. Salting involves adding a unique, random value to each password before hashing, which prevents attackers from using precomputed tables, or "rainbow tables," to crack passwords efficiently. Additionally, the use of modern, brute-force-resistant hashing algorithms significantly increases the time and computational resources required for an attacker to guess passwords. By implementing these best practices, organisations can strengthen their defences against potential breaches and better protect user credentials from evolving threats in an increasingly hostile digital environment.

Finally, access to servers, both remote and physical, is restricted to **authorised personnel** only, to safeguard (sensitive) data and maintain the integrity of the system. Implementing a robust access control policy ensures that only individuals with the appropriate permissions can interact with server environments, reducing the risk of unauthorised access and potential data breaches. This principle of least privilege not only protects critical infrastructure but also enhances accountability. Regular audits and reviews of access permissions can be used to ensure that only current, legitimate users retain access, thereby reinforcing security measures and minimising vulnerabilities.

The following sections present more information on how the specific tools and dashboards of COMPAIR handled compliance. They can be used as a reference for future CS and initiatives that are providing similar tools, but also for decision making tools in general.

3.4.1. Policy Monitoring Dashboard (PMD)

The Policy Monitoring Dashboard (PMD) helps users explore the different sensors that are deployed in the project in what is called "Browse mode". In "Project Mode", administrators can create a dashboard for a specific project that enables assessing the changes in traffic and air pollution after implementing a policy change. A set of graphs shows the before and after situation, as well as the delta.

***Table 2**: Policy Monitoring Dashboard approach to personal data protection*

Category of Measures	Approach
Technical measures to safeguard the rights and freedoms of the data subjects	• No data from end users is used or stored in the PMD (acting as a standalone component) • Sensors are not shown on the exact location, but in a hexagon that shows approximate location
Organisational measures to safeguard the rights	Terms and conditions are available in the PMD page. We consider that the user complies with these terms and

and freedoms of the data subjects	conditions in order to use the functionalities of the tool.
Privacy policy	Privacy policy of the COMPAIR project reflects the rules and the requirements of the GDPR and has been approved by the COMPAIR partners. Additionally, a specific policy for the PMD captures all the necessary information that needs to be communicated to the end-users of the tool.
Security measures to prevent unauthorised access to personal data or the equipment used for processing	Despite the fact that no personal data are stored by PMD, several security measures are taken in order to prevent unauthorised access, some of which are: ● Use of firewalls to prevent unauthorised access to the server where PMD is running ● Use of secure communication protocols in any data exchange ● Use of credentials to access the server
Anonymisation or pseudonymisation techniques	Not applicable since no personal data is being processed.
Relevance and limitation of data processing for goals and purposes of the COMPAIR project	Not applicable since no personal data is being processed.

3.4.2. Carbon Footprint Simulation Dashboard (CO2 Dashboard)

The purpose of the Carbon Footprint Simulation Dashboard (CO2) is to guide users to improve their behaviours through more environmentally friendly choices, regarding their carbon footprint. It consists of two tools, the Carbon Footprint Calculator and the Simulation Dashboard. The Carbon Footprint Calculator allows the user to calculate their carbon footprint through a series of questions regarding their daily habits (such as transportation habits, use of electricity, etc). In the end, the user is presented with their carbon footprint and a comparison between the result, their country's average, and the EU average. They also receive recommendations on how they can improve their carbon footprint, along with informational links.

The second tool is the Scenario Simulation Dashboard. This tool allows citizens to participate in policy making by submitting their opinion in the form of scenarios regarding a specific quantified environmental goal. It presents a set of actions they are willing to make, as well as actions they are willing to accept from the government with the purpose of reducing carbon emissions. Citizens can choose among three types of actions; actions they are willing to adopt, actions they are willing to accept from the central government, and actions they are willing to accept from the local government.

The types of data that are used for the Carbon Footprint Simulation Dashboard are the following:

Demographic data:

- Country
- City
- Gender
- Age (age group)
- Social Aid
- Education level
- Municipal Community

Carbon Footprint Calculator Data:

- Distance travelled with a vehicle, consumption of vehicle (litres/100km, kWh/100km), vehicle's type of fuel.
- Number of flights, duration of flights, average distance of flights.
- Number of train trips per year
- Average distance of train trip
- Building's fuel consumption
- Type of fuel used in building
- Electricity used in building
- Use of solar panels for water heating (solar thermal)
- Use of heat pump
- Energy efficiency of appliances (refrigerator, washing machine, dishwasher, oven)
- Data on waste management (amount of recycling and composting).

Scenario Simulation Data:

- Opinion on personal actions that could reduce Greenhouse Gas Emissions
- Opinion on government actions that could reduce Greenhouse Gas Emissions
- Opinion on local government actions that could reduce Greenhouse Gas Emissions

***Table 3**: Carbon Footprint Simulation Dashboard approach to personal data protection*

Category of Measures	Approach
Technical measures to safeguard the rights and freedoms of the data subjects	• There are two ways for the end users (citizens) to interact with the CO2 Dashboard: ○ Without login: The end user can anonymously interact with the two tools available on the CO2 Dashboard. The research data will be collected and stored but there will be no user ID to associate with the user manager. ○ With login: The end user will use their account to login to the CO2 Dashboard in order to use the two available tools. The research data will be collected and stored and there will be a user ID to associate these data with the user manager.
Organisational measures to safeguard the rights and freedoms of the data subjects	A **consent policy** will be accepted or declined by the individual. This policy specifies the subject matter of the processing, the duration of the processing, the nature and the purpose of the processing, the type of personal data involved, the data controller's (COMPAIR project) obligations and rights.
Privacy Policy	The Privacy Policy of the COMPAIR project reflects the rules and the requirements of the GDPR and has been approved by

	the COMPAIR partners. Additionally, a specific policy for the CO2 Dashboard captures all the necessary information that needs to be communicated to the end-users of the tool.
Security measures to prevent unauthorised access to personal data or the equipment used for processing	No personal data is stored on the server of the Dashboard. Only the user's ID is stored, which can only be associated with the user's data stored in the user manager. Additionally, only authorised COMPAIR partners have access to the collected personal data. Policy makers and other users who will use the dashboard will only have access to aggregated and statistical data.
Anonymisation or pseudonymisation techniques	Not applicable since no personal data is being processed.
Relevance and limitation of data processing for goals and purposes of the COMPAIR project	The Demographic Data (aggregated data, without containing any personal data) is used by the Pilot Partners to identify the low SES groups that are using the CO2 Dashboard. The Carbon Footprint Calculator Data is used to calculate the end users' carbon footprint so that they can be informed on their current status, as well as receive recommendations on how they can improve their habits to reduce their emissions. The Scenario Simulation Data is used as aggregate data for policy-makers to make more informed decisions.

3.4.3. Citizen Science Dynamic Exposure Visualisation Application

As an augmented reality app, the Dynamic Exposure Visualisation Application (DEVA) aims to raise awareness of and spur interest in increasing ambient air quality by visualising air pollution from the local environment on a 2D surface of a smartphone or tablet. More than just displaying local air pollution, it encourages users to explore air quality on their daily routes by engaging with the app's various features, such as the pollution hotspot warning system. DEVA targets laypeople (citizens, parents, children, etc.) and researchers alike by offering a set of functionalities and simple gamification tools aimed at driving the engagement of different target groups.

The app comes in three different modes: an exploration mode, an expert mode, and a trip recording mode. The exploration mode is primarily geared toward school children and requires minimal configuration for the app to be used. The expert mode, on the other hand, is mainly meant to be used by administrators who want to experiment with different visualisation, GPS and other settings to get the most out of the app.

Finally, the trip recorder works in conjunction with the Dynamic Exposure Visualisation Dashboard (DEV-D). Users who measure air quality with their SODAQ devices can use DEVA to enter their device's ID and have their trip and measured air quality data be displayed in the DEV-D. By using the users' GPS data to more accurately display air

pollution, DEVA also offers features where citizens can input data on the type of transportation they used at a given time. This data, in turn, is used as a key source for mapping information about mobile measurements in the DEV-D.

DEVA has collected the following user data:

- GPS information of DEVA users
- User name
- User height (for calibration purposes)

The data collected by DEVA is saved on the device. Only the GPS position is transferred to the data manager and to other web services in order to request the desired sensor data..

***Table 4**: Citizen Science Dynamic Exposure Visualisation Application approach to personal data protection*

Category of Measures	Approach
Technical measures to safeguard the rights and freedoms of the data subjects	Users can access DEVA either anonymously (exploration mode) or pseudo-anonymously (via username in expert mode). ● **Exploration mode**: The user can start using the app without a need to provide a username. ● **Expert mode**: The user will provide a username to create a profile. The username is required to ensure that custom settings are saved and don't have to be reconfigured every time the app is used. ● **Trip recorder:** Only SODAQ's IMEI will be provided to the data manager and not the device code. This ensures that a SODAQ device cannot be traced back to individual users.
Organisational measures to safeguard the rights and freedoms of the data subjects	A **consent policy** will be accepted or declined by the individual. This policy specifies the subject matter of the processing, the duration of the processing, the nature and the purpose of the processing, the type of personal data involved, and the data controller's (COMPAIR project) obligations and rights.
Privacy policy	Privacy policy of the COMPAIR project reflects the rules and the requirements of the GDPR and has been approved by the COMPAIR partners. Additionally, a specific policy for the DEVA and DEV-D captures all the necessary information that needs to be communicated to the end-users of the tool.
Security measures to prevent unauthorised access to personal data or the equipment used for processing	User profiles are saved in the local app memory space and are protected from external views as any other user data. The sensitive data in user profile are name and height. The last trip is saved in the save memory area and transferred to the data manager after finishing the trip. Right after, the trip data are deleted on the device.

Anonymisation or pseudonymisation techniques	There are no further techniques like this.
Relevance and limitation of data processing for goals and purposes of the COMPAIR project	Air quality and traffic data produced by citizen sensors and displayed in DEVA is used for gamification and educational purposes. The aim is to encourage air quality exploration in the user's area, prompting them to learn more about air quality.

4. Handling of vulnerable groups

In order for the results of a project to be objective and inclusive, pilot campaigns should be designed in a way that they capture a broader set of participants, including citizens from different SES groups (including also the more vulnerable and lower SES groups – such as children, elderly people, and minorities).

According to the guidelines of the European Commission[6],[7], when vulnerable groups are included in research, it is important to guarantee safe conditions for their participation.

The previous sections of this deliverable presented all the relevant technical and organisational measures that can be implemented to satisfy all legal requirements that the European legislation imposes.

One important lesson, for the projects' partners, and a hint for future readers / researchers is that the re-use of existing knowledge is always welcomed. The Flanders pilot test case (described in detail in deliverables D5.4 "Open Round Report" and D5.6: "Public Round Report") was **able to include SES groups, without having to collect / process special categories (sensitive) of personal data**. This was realised by making use of existing information: They had collected relevant data in past projects (purposes). This personal data couldn't be used for other purposes, of course, however aggregated anonymous statistical data had been deducted and could be used elsewhere. Flanders pilot test case knows what percentage of their population is of a particular group (say minors) and, thus, how effective their campaign would be on raising awareness among minors (and, consequently, their families).

The processes mentioned above could be used as a recommendation in future research projects. The researchers could have an overview of the available data they have access to, to find potential alternative ways to exploit them efficiently and use them in such a way that the results of the research can still be accurate and of value.

[6] Ethics in Social Science and Humanities, European Commission, 2021, available online at https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ethics-in-social-science-and-humanities_he_en.pdf

[7] Ethics and data protection, European Commission, 2021, available online at https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ethics-and-data-protection_he_en.pdf

5. Conclusions

In conclusion, as every initiative should, COMPAIR has meticulously examined the relevant legislation, with a primary focus on the General Data Protection Regulation (GDPR), to ensure full compliance in its operations. Through a thorough analysis of the GDPR's requirements, we have implemented best practices for data protection, emphasising transparency, user consent, and data integrity. The project's commitment to adhering to these legal frameworks not only safeguards the personal information of our stakeholders but also reinforces our dedication to ethical standards in data management.

The project was led by privacy by design principles to ensure data minimization and secure storage, with comprehensive consent forms and privacy policies to inform participants about the use of their data. In addition, all pilot campaigns were carefully designed to respect participants' rights and ensure compliance with GDPR regulations.

This document presented all these legal requirements, best practices, and most importantly lessons learned, to be used in future CS and initiatives as a starting point in their attempt to reach compliance. By aligning their practices with the principles of the GDPR, they will not only fulfil their legal obligations but also foster trust and confidence among their users, partners, and stakeholders, paving the way for a responsible and sustainable approach to data privacy in the digital age.

6. References

Brunotte, W., Chazette, L., Kohler, L., Klunder, J., & Schneider, K. (2022, May). What about my privacy? Helping users understand online privacy policies. In Proceedings of the International Conference on Software and System Processes and International Conference on Global Software Engineering (pp. 56-65).

Bygrave, L. A. (2022). Security by design: Aspirations and realities in a regulatory context. Oslo Law Review, (3), 126-177.

Diamantopoulou, Vasiliki, Costas Lambrinoudakis, Jennifer King, and Stefanos Gritzalis. "EU GDPR: Toward a Regulatory Initiative for Deploying a Private Digital Era." (2022): 427-448.
Ebad, S. A. (2022). Exploring how to apply secure software design principles. IEEE Access, 10, 128983-128993.

European Commission, 2018: Ethics and Data Protection, available online at https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-data-protection_en.pdf

European Commission, 2020: Communication from the Commission Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection 2020/C 124 I/01, available online at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020XC0417%2808%29

Luehnen, J., Muehlhauser, I., & Steckelberg, A. (2018). The quality of informed consent forms—a systematic review and critical analysis. Deutsches Aerzteblatt International, 115(22), 377.

NIST (2014). Richard Kissel, Andrew Regenscheid, Matthew Scholl, Kevin Stine. Guidelines for Media Sanitization, http://dx.doi.org/10.6028/NIST.SP.800-88r1

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), available online at https://eur-lex.europa.eu/eli/reg/2016/679/oj

7. Annex - Consent Forms

Athens Consent Form

PARTICIPATION FORM & PRIVACY POLICY

I. ABOUT THE RESEARCH PROJECT

1. COMPAIR EU-funded Project

COMPAIR is an EU Innovation Action (IA) project. Its main focus will be on bolstering citizens' capacity to monitor, understand, and change their environmental impact, both at a behavioural and policy level. It unlocks the power of the wider public, including people from lower-socio economic groups, to provide broad granular data around a central theme of air quality, complementing and improving the quality of official datasets and making new information useful for research purposes, policy making and behavioural change.

The COMPAIR project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101036563. The COMPAIR project started on 1 November 2021 and has a duration of 36 months.

2. Research aspects

The Athens pilot, in the COMPAIR project focuses on the engagement of citizens in participating in the behavioural change towards a reduced carbon footprint and better air-quality. These two dimensions are going to be achieved through the development of a CO2 Simulation Dashboard and the distribution of air quality sensors. In this section, a detailed description on senior citizens' engagement and sensor distribution will follow and report on activities included in open round testing. The main objective of the open round in Athens is to raise awareness on air quality among citizens targeting elderly inhabitants in the area of Neos Kosmos, selected after internal discussions with the Municipality of Athens.

3. Project Partners

The partners of the COMPAIR project are the following:

	Organisation Name	Country
1	VLAAMSE GEWEST (Project coordinator)	Belgium
2	IS-PRACTICE BVBA	Belgium
3	ATHENS TECHNOLOGY CENTER ANONYMI VIOMICHANIKI EMPORIKI KAI TECHNIKI ETAIREIA EFARMOGON YPSILIS TECHNOLOGIAS	Greece
4	INTER 3 GMBH INSTITUT FUR RESSOURCENMANAGEMENT	Germany
5	21C CONSULTANCY LIMITED	United Kingdom
6	DIMOS ATHINAION EPICHEIRISI MICHANOGRAFISIS	Greece
7	ENERGY AGENCY OF PLOVDIV ASSOCIATION	Bulgaria

8	VEREIN DER EUROPAEISCHEN BURGERWISSENSCHAFTEN - ECSA E.V.	Germany
9	FRAUNHOFER GESELLSCHAFT ZUR FOERDERUNG DER ANGEWANDTEN FORSCHUNG E.V.	Germany
10	STICHTING IMEC NEDERLAND	Netherlands
11	ASSOTSIATSIA ZA RAZVITIE NA SOFIA	Bulgaria
12	SODAQ HOLDING BV	Netherlands
13	REAR WINDOW	Belgium
14	PANEPISTIMIO AIGAIOU	Greece
15	VLAAMSE MILIEUMAATSCHAPPIJ	Belgium

4. Project contact details

Coordinator	Technical Specialists
Lieven Raes lieven.raes@vlaanderen.be	Project Manager: Marina Klitsi (m.klitsi@atc.gr) Technical Manager: Sakis Dalianis (T.Dalianis@atc.gr)

II. ABOUT THE RESEARCH PARTICIPANT

In the event you would like to participate in the Research, please provide us with the following information, which will be processed in accordance with the below Privacy Policy:

First name _____

Last name _____

Email address _____

III. RESEARCH CONSENT

I volunteer to participate in the Research described above conducted in the context of the COMPAIR Project.	Yes	No
I understand that my participation is voluntary (my choice).	Yes	No
I understand that I will not receive any financial compensation for my participation.	Yes	No
I am aware that I have the right to withdraw from the Research at any time in the Project.	Yes	No
I have read and understood the explanation provided to me about the Project.	Yes	No
I have read and understood the Privacy Policy and I understand that my personal data will be processed as described in the Privacy Policy.	Yes	No
I agree to have my role and/or organisation mentioned in the reports, including public reports, to be submitted to the European Commission and published online.	Yes	No
I have had all my questions answered to my satisfaction.	Yes	No
I know who to contact if I have any question about the Project and my privacy.	Yes	No
I have been given a copy of this participation form.	Yes	No

First name _____

Last name _____

Signature _____

Date _____ City / Town_____

IV. PRIVACY POLICY

1. Scope of this policy

This Privacy Policy describes how your personal data is collected, used and otherwise processed in the context of the EU COMPAIR Project funded under the H2020 research programme, contract no. H2020-101036563 (hereafter the "**Project**").

This Privacy Policy includes a description of your data protection rights, including a right to object to some of the processing activities we carry out.

In this Privacy Policy:

- "**We**" or "**us**" refer to the Partners of the COMPAIR Project listed in Section I.3. above, who will process your personal data as data controllers and as described herein.
- "**Data Protection Legislation**" means the Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the "**GDPR**"), as well as any legislation and/or regulation implemented or created pursuant to the GDPR and the e-Privacy legislation, or which amends, replaces, re-enacts or consolidates any of them, and all other national applicable laws relating to processing of personal data and privacy that may exist under applicable law.
- The terms "controller", "processor", "third party", "supervisory authority", "personal data", "processing", "data subject", shall have the meanings set out in the applicable Data Protection Legislation.

2. What personal data is processed?

In the context of the Project, your personal data is processed by the Athens Partners, as follows:

- **Processing purpose(s):** for the purpose of carrying out the research in the COMPAIR Project, as described in Section I above.
- **Processed data categories:** first name, last name, email address, age group (only above or below 65), selection among two areas (i.e. Kipseli or Neos Kosmos).
- **Source of data:** from the participant, directly.
- **Legal basis:** Our legitimate interests. It is in the Partners' legitimate interests to process your personal data as a Research participant. We will always make sure that your interests are safeguarded. This does not affect your rights, as described below.

3. How long is your personal data stored?

We retain your personal data for as long as is required to fulfil the activities set out in the Participation Form and this Privacy Policy, for as long as otherwise communicated to you or for as long as is permitted by applicable law. For example, we may retain your personal data if it is reasonably necessary to comply with any legal obligations, meet any regulatory requirements, resolve any disputes or litigation, or as otherwise needed to enforce this

Privacy Policy and prevent fraud and abuse. This period will last until October 2024, by the end of the project.

4. **How is your personal data shared with third parties?**

The data that we collect from you as described in this Privacy Policy will not be shared with any third parties.

5. **Is your personal data transferred outside the European Economic Area (EEA)?**

The data that we collect from you as described in this Privacy Policy will not be transferred to and stored at a destination outside the EEA.

6. **What are your rights?**

Once you have provided your personal data, several rights are recognized under the Data Protection Legislation, which you can in principle exercise free of charge, subject to statutory exceptions. In particular, you have the following rights:

- **Right to access, review, and rectify your data:** you have the right to access, review, and rectify your personal data. You may be entitled to ask us for a copy of your information, to review or correct it if you wish to review or rectify any information. You may also request a copy of the personal data processed as described herein by sending an email to ethics@wecompair.eu. You can access and review this information and, if necessary, ask to rectify your information.
- **Right to erasure:** you have the right to erasure of all the personal data processed by as described herein in case it is no longer needed for the purposes for which the personal data was initially collected or processed, in accordance with the Data Protection Legislation.
- **Right to object or restriction of processing:** under certain circumstances described in the Data Protection Legislation, you may ask for a restriction of processing or object to the processing of your personal data.
- **Right to data portability**: you have the right to receive the Personal Data processed in a format which is structured, commonly used and machine-readable and to transmit this data to another service provider.

These rights may be limited, for example if fulfilling your request would reveal personal data about another person, or if you ask us to delete information which we are required by law to keep or have compelling legitimate interests in keeping.
To exercise any of these rights, you can get in touch with us using the details set out below. If you have unresolved concerns, you have the right to lodge a complaint with an EU data protection authority where you live, work or where you believe a breach may have occurred.

7. **What security measures are put in place?**

Appropriate technical and organisational measures are implemented in order to ensure an appropriate level of security of your personal data.
In the event personal information is compromised as a result of a security breach and where the breach is likely to result in a high risk to your rights and freedoms, we will make the necessary notifications, as required under the Data Protection Legislation.

8. **How can we be contacted?**

Questions, comments, remarks, requests or complaints regarding this Privacy Policy are welcome and should be addressed to ethics@wecompair.eu.

Berlin Consent Form

PARTICIPATION FORM & PRIVACY POLICY

I. ABOUT THE RESEARCH PROJECT

1. COMPAIR EU-funded Project

COMPAIR is an EU Innovation Action (IA) project. Its main focus will be on bolstering citizens' capacity to monitor, understand, and change their environmental impact, both at a behavioural and policy level. It unlocks the power of the wider public, including people from lower-socio economic groups, to provide broad granular data around a central theme of air quality, complementing and improving the quality of official datasets and making new information useful for research purposes, policy making and behavioural change.
The COMPAIR project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101036563. The COMPAIR project started on 1 November 2021 and has a duration of 36 months.

2. Research aspects

The Berlin pilot in the COMPAIR project focuses on air quality measurements, which will be conducted by an extensive network of high-end measurement stations located across the city, encompassing different types of urban topographies. The aim of these measurements is to ascertain the exposure of cyclists and school children on their way to school/work, evaluating both spontaneous and “helped" behavioural change. Spontaneous behavioural change refers to citizens changing their behaviour based on their access to the most basic data on PM pollution along their commute routes. “Helped” change, on the other hand, is more informative and provides, along with information on individual and cumulative exposures, a set of recommendations to adopt more healthy behavioural patterns. The overarching aim is to carry this experience to other cyclists and schools across Berlin.

3. Project Partners

The partners of the COMPAIR project are the following:

	Organisation Name	Country
1	VLAAMSE GEWEST (Project coordinator)	Belgium
2	IS-PRACTICE BVBA	Belgium
3	ATHENS TECHNOLOGY CENTER ANONYMI VIOMICHANIKI EMPORIKI KAI TECHNIKI ETAIREIA EFARMOGON YPSILIS TECHNOLOGIAS	Greece
4	INTER 3 GMBH INSTITUT FUR RESSOURCENMANAGEMENT	Germany
5	21C CONSULTANCY LIMITED	United Kingdom
6	DIMOS ATHINAION EPICHEIRISI MICHANOGRAFISIS	Greece

7	ENERGY AGENCY OF PLOVDIV ASSOCIATION	Bulgaria
8	VEREIN DER EUROPAEISCHEN BURGERWISSENSCHAFTEN - ECSA E.V.	Germany
9	FRAUNHOFER GESELLSCHAFT ZUR FOERDERUNG DER ANGEWANDTEN FORSCHUNG E.V.	Germany
10	STICHTING IMEC NEDERLAND	Netherlands
11	ASSOTSIATSIA ZA RAZVITIE NA SOFIA	Bulgaria
12	SODAQ HOLDING BV	Netherlands
13	REAR WINDOW	Belgium
14	PANEPISTIMIO AIGAIOU	Greece
15	VLAAMSE MILIEUMAATSCHAPPIJ	Belgium

4. Project contact details

Coordinator	**Technical Specialists**
Lieven Raes lieven.raes@vlaanderen.be	**Project Manager: Marina Klitsi** (m.klitsi@atc.gr) Technical Manager: Sakis Dalianis (T.Dalianis@atc.gr)

II. ABOUT THE RESEARCH PARTICIPANT

In the event you would like to participate in the Research, please provide us with the following information, which will be processed in accordance with the below Privacy Policy:

First name _____

Last name _____

Email address _____

III. RESEARCH CONSENT

I volunteer to participate in the Research described above conducted in the context of the COMPAIR Project.	Yes	No
I understand that my participation is voluntary (my choice).	Yes	No
I understand that I will not receive any financial compensation for my participation.	Yes	No
I am aware that I have the right to withdraw from the Research at any time in the Project.	Yes	No
I have read and understood the explanation provided to me about the Project.	Yes	No
I have read and understood the Privacy Policy and I understand that my personal data will be processed as described in the Privacy Policy.	Yes	No
I agree to have my role and/or organisation mentioned in the reports, including public reports, to be submitted to the European Commission and published online.	Yes	No
I have had all my questions answered to my satisfaction.	Yes	No
I know who to contact if I have any question about the Project and my privacy.	Yes	No
I have been given a copy of this participation form.	Yes	No

First name _____

Last name _____

Signature _____

Date _____ City / Town _____

IV. PRIVACY POLICY

1. Scope of this policy

This Privacy Policy describes how your personal data is collected, used and otherwise processed in the context of the EU COMPAIR Project funded under the H2020 research programme, contract no. H2020-101036563 (hereafter the "Project").

This Privacy Policy includes a description of your data protection rights, including a right to object to some of the processing activities we carry out.

In this Privacy Policy:

- **"We"** or **"us"** refer to the Partners of the COMPAIR Project listed in Section I.3. above, who will process your personal data as data controllers and as described herein.
- **"Data Protection Legislation"** means the Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the "**GDPR**"), as well as any legislation and/or regulation implemented or created pursuant to the GDPR and the e-Privacy legislation, or which amends, replaces, re-enacts or consolidates any of them, and all other national applicable laws relating to processing of personal data and privacy that may exist under applicable law.
- The terms "controller", "processor", "third party", "supervisory authority", "personal data", "processing", "data subject", shall have the meanings set out in the applicable Data Protection Legislation.

2. What personal data is processed?

In the context of the Project, your personal data is processed by the Berlin Partners, as follows:

- **Processing purpose(s):** for the purpose of carrying out the research in the COMPAIR Project, as described in Section I above.
- **Processed data categories:** first name, last name, age, gender, height, educational level, mother tongue, email address, IP address, physical address (including floor), GPS coordinates.
- **Source of data:** from the participant, directly.
- **Legal basis:** Our legitimate interests. It is in the Partners' legitimate interests to process your personal data as a Research participant. We will always make sure that your interests are safeguarded. This does not affect your rights, as described below.

3. How long is your personal data stored?

We retain your personal data for as long as is required to fulfil the activities set out in the Participation Form and this Privacy Policy, for as long as otherwise communicated to you or for as long as is permitted by applicable law. For example, we may retain your personal data if it is reasonably necessary to comply with any legal obligations, meet any regulatory

requirements, resolve any disputes or litigation, or as otherwise needed to enforce this Privacy Policy and prevent fraud and abuse. This period will last until October 2024, by the end of the project.

4. How is your personal data shared with third parties?

The data that we collect from you as described in this Privacy Policy will not be shared with any third parties.

5. Is your personal data transferred outside the European Economic Area (EEA)?

The data that we collect from you as described in this Privacy Policy will not be transferred to and stored at a destination outside the EEA.

6. What are your rights?

Once you have provided your personal data, several rights are recognized under the Data Protection Legislation, which you can in principle exercise free of charge, subject to statutory exceptions. In particular, you have the following rights:

- **Right to access, review, and rectify your data:** you have the right to access, review, and rectify your personal data. You may be entitled to ask us for a copy of your information, to review or correct it if you wish to review or rectify any information. You may also request a copy of the personal data processed as described herein by sending an email to ethics@wecompair.eu. You can access and review this information and, if necessary, ask to rectify your information.
- **Right to erasure:** you have the right to erasure of all the personal data processed by as described herein in case it is no longer needed for the purposes for which the personal data was initially collected or processed, in accordance with the Data Protection Legislation.
- **Right to object or restriction of processing:** under certain circumstances described in the Data Protection Legislation, you may ask for a restriction of processing or object to the processing of your personal data.
- **Right to data portability:** you have the right to receive the Personal Data processed in a format which is structured, commonly used and machine-readable and to transmit this data to another service provider.

These rights may be limited, for example if fulfilling your request would reveal personal data about another person, or if you ask us to delete information which we are required by law to keep or have compelling legitimate interests in keeping.
To exercise any of these rights, you can get in touch with us using the details set out below. If you have unresolved concerns, you have the right to lodge a complaint with an EU data protection authority where you live, work or where you believe a breach may have occurred.

7. What security measures are put in place?

Appropriate technical and organisational measures are implemented in order to ensure an appropriate level of security of your personal data.
In the event personal information is compromised as a result of a security breach and where the breach is likely to result in a high risk to your rights and freedoms, we will make the necessary notifications, as required under the Data Protection Legislation.

8. How can we be contacted?

Questions, comments, remarks, requests or complaints regarding this Privacy Policy are welcome and should be addressed to ethics@wecompair.eu.

Flanders Consent Form

PARTICIPATION FORM & PRIVACY POLICY

I. ABOUT THE RESEARCH PROJECT

1. COMPAIR EU-funded Project

COMPAIR is an EU Innovation Action (IA) project. Its main focus will be on bolstering citizens' capacity to monitor, understand, and change their environmental impact, both at a behavioural and policy level. It unlocks the power of the wider public, including people from lower-socio economic groups, to provide broad granular data around a central theme of air quality, complementing and improving the quality of official datasets and making new information useful for research purposes, policy making and behavioural change.

The COMPAIR project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101036563. The COMPAIR project started on 1 November 2021 and has a duration of 36 months.

2. Research aspects

The Flanders pilot in the COMPAIR project aims to demonstrate the impact of the traffic in the streets around a school on air pollution and air quality. For this research, two pilots will take place, i) demonstrating the impact of a school street on traffic and air quality in Herzele, and ii) demonstrating the impact of a mobility plan on traffic and air quality in Ghent. These pilots will provide useful insight regarding the effect on air pollution in relation to the traffic around the school and if the rise or decline of traffic can lead to a discernible change in air quality.

3. Project Partners

The partners of the COMPAIR project are the following:

	Organisation Name	Country
1	VLAAMSE GEWEST (Project coordinator)	Belgium
2	IS-PRACTICE BVBA	Belgium
3	ATHENS TECHNOLOGY CENTER ANONYMI VIOMICHANIKI EMPORIKI KAI TECHNIKI ETAIREIA EFARMOGON YPSILIS TECHNOLOGIAS	Greece
4	INTER 3 GMBH INSTITUT FUR RESSOURCENMANAGEMENT	Germany
5	21C CONSULTANCY LIMITED	United Kingdom
6	DIMOS ATHINAION EPICHEIRISI MICHANOGRAFISIS	Greece
7	ENERGY AGENCY OF PLOVDIV ASSOCIATION	Bulgaria

8	VEREIN DER EUROPAEISCHEN BURGERWISSENSCHAFTEN - ECSA E.V.	Germany
9	FRAUNHOFER GESELLSCHAFT ZUR FOERDERUNG DER ANGEWANDTEN FORSCHUNG E.V.	Germany
10	STICHTING IMEC NEDERLAND	Netherlands
11	ASSOTSIATSIA ZA RAZVITIE NA SOFIA	Bulgaria
12	SODAQ HOLDING BV	Netherlands
13	REAR WINDOW	Belgium
14	PANEPISTIMIO AIGAIOU	Greece
15	VLAAMSE MILIEUMAATSCHAPPIJ	Belgium

4. Project contact details

Coordinator	Technical Specialists
Lieven Raes lieven.raes@vlaanderen.be	Project Manager: Marina Klitsi (m.klitsi@atc.gr) Technical Manager: Sakis Dalianis (T.Dalianis@atc.gr)

II. ABOUT THE RESEARCH PARTICIPANT

In the event you would like to participate in the Research, please provide us with the following information, which will be processed in accordance with the below Privacy Policy:

First name _____

Last name _____

Email address _____

III. RESEARCH CONSENT

I volunteer to participate in the Research described above conducted in the context of the COMPAIR Project.	Yes	No
I understand that my participation is voluntary (my choice).	Yes	No
I understand that I will not receive any financial compensation for my participation.	Yes	No
I am aware that I have the right to withdraw from the Research at any time in the Project.	Yes	No
I have read and understood the explanation provided to me about the Project.	Yes	No
I have read and understood the Privacy Policy and I understand that my personal data will be processed as described in the Privacy Policy.	Yes	No
I agree to have my role and/or organisation mentioned in the reports, including public reports, to be submitted to the European Commission and published online.	Yes	No
I have had all my questions answered to my satisfaction.	Yes	No
I know who to contact if I have any question about the Project and my privacy.	Yes	No
I have been given a copy of this participation form.	Yes	No

First name _____

Last name _____

Signature _____

Date _____ City / Town _____

IV. PRIVACY POLICY

1. Scope of this policy

This Privacy Policy describes how your personal data is collected, used and otherwise processed in the context of the EU COMPAIR Project funded under the H2020 research programme, contract no. H2020-101036563 (hereafter the "**Project**").

This Privacy Policy includes a description of your data protection rights, including a right to object to some of the processing activities we carry out.

In this Privacy Policy:

- "**We**" or "**us**" refer to the Partners of the COMPAIR Project listed in Section I.3. above, who will process your personal data as data controllers and as described herein.
- "**Data Protection Legislation**" means the Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the "**GDPR**"), as well as any legislation and/or regulation implemented or created pursuant to the GDPR and the e-Privacy legislation, or which amends, replaces, re-enacts or consolidates any of them, and all other national applicable laws relating to processing of personal data and privacy that may exist under applicable law.
- The terms "controller", "processor", "third party", "supervisory authority", "personal data", "processing", "data subject", shall have the meanings set out in the applicable Data Protection Legislation.

2. What personal data is processed?

In the context of the Project, your personal data is processed by the Flanders Partners, as follows:

- **Processing purpose(s):** for the purpose of carrying out the research in the COMPAIR Project, as described in Section I above.
- **Processed data categories:** sex, age, location of living.
- **Source of data:** from the participant, directly.
- **Legal basis:** Our legitimate interests. It is in the Partners' legitimate interests to process your personal data as a Research participant. We will always make sure that your interests are safeguarded. This does not affect your rights, as described below.

We rely on the following organisations to process your personal data:

Organisation (data processor)	Processed data categories	Instructions
Google Drive suite	sex, age, location of living	Storing and processing of data.

3. How long is your personal data stored?

We retain your personal data for as long as is required to fulfil the activities set out in the Participation Form and this Privacy Policy, for as long as otherwise communicated to you or for as long as is permitted by applicable law. For example, we may retain your personal data if it is reasonably necessary to comply with any legal obligations, meet any regulatory requirements, resolve any disputes or litigation, or as otherwise needed to enforce this Privacy Policy and prevent fraud and abuse. This period will last until October 2024, by the end of the project.

4. How is your personal data shared with third parties?

The data that we collect from you as described in this Privacy Policy will not be shared with any third parties.

5. Is your personal data transferred outside the European Economic Area (EEA)?

The data that we collect from you as described in this Privacy Policy will not be transferred to and stored at a destination outside the EEA.

6. What are your rights?

Once you have provided your personal data, several rights are recognized under the Data Protection Legislation, which you can in principle exercise free of charge, subject to statutory exceptions. In particular, you have the following rights:

- **Right to access, review, and rectify your data:** you have the right to access, review, and rectify your personal data. You may be entitled to ask us for a copy of your information, to review or correct it if you wish to review or rectify any information. You may also request a copy of the personal data processed as described herein by sending an email to ethics@wecompair.eu. You can access and review this information and, if necessary, ask to rectify your information.
- **Right to erasure:** you have the right to erasure of all the personal data processed by as described herein in case it is no longer needed for the purposes for which the personal data was initially collected or processed, in accordance with the Data Protection Legislation.
- **Right to object or restriction of processing:** under certain circumstances described in the Data Protection Legislation, you may ask for a restriction of processing or object to the processing of your personal data.
- **Right to data portability**: you have the right to receive the Personal Data processed in a format which is structured, commonly used and machine-readable and to transmit this data to another service provider.

These rights may be limited, for example if fulfilling your request would reveal personal data about another person, or if you ask us to delete information which we are required by law to keep or have compelling legitimate interests in keeping.
To exercise any of these rights, you can get in touch with us using the details set out below. If you have unresolved concerns, you have the right to lodge a complaint with an EU data protection authority where you live, work or where you believe a breach may have occurred.

7. What security measures are put in place?

Appropriate technical and organisational measures are implemented in order to ensure an appropriate level of security of your personal data.

In the event personal information is compromised as a result of a security breach and where the breach is likely to result in a high risk to your rights and freedoms, we will make the necessary notifications, as required under the Data Protection Legislation.

8. How can we be contacted?

Questions, comments, remarks, requests or complaints regarding this Privacy Policy are welcome and should be addressed to ethics@wecompair.eu.

Plovdiv Consent Form

PARTICIPATION FORM & PRIVACY POLICY

I. ABOUT THE RESEARCH PROJECT

1. COMPAIR EU-funded Project

COMPAIR is an EU Innovation Action (IA) project. Its main focus will be on bolstering citizens' capacity to monitor, understand, and change their environmental impact, both at a behavioural and policy level. It unlocks the power of the wider public, including people from lower-socio economic groups, to provide broad granular data around a central theme of air quality, complementing and improving the quality of official datasets and making new information useful for research purposes, policy making and behavioural change.

The COMPAIR project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101036563. The COMPAIR project started on 1 November 2021 and has a duration of 36 months.

2. Research aspects

The Plovdiv pilot, in the frame of COMPAIR project, tries to show the connection between traffic intensity and levels of PM and NO2 around the schools. Exposure to air pollution is a significant risk to children's health. The students and volunteers were involved in air quality and traffic measurements. The main goal of the open round in Plovdiv is to raise awareness of air quality around schools and to find a way for improvements.

3. Project Partners

The partners of the COMPAIR project are the following:

	Organisation Name	Country
1	VLAAMSE GEWEST (Project coordinator)	Belgium
2	IS-PRACTICE BVBA	Belgium
3	ATHENS TECHNOLOGY CENTER ANONYMI VIOMICHANIKI EMPORIKI KAI TECHNIKI ETAIREIA EFARMOGON YPSILIS TECHNOLOGIAS	Greece
4	INTER 3 GMBH INSTITUT FUR RESSOURCENMANAGEMENT	Germany
5	21C CONSULTANCY LIMITED	United Kingdom
6	DIMOS ATHINAION EPICHEIRISI MICHANOGRAFISIS	Greece

7	ENERGY AGENCY OF PLOVDIV ASSOCIATION	Bulgaria
8	VEREIN DER EUROPAEISCHEN BURGERWISSENSCHAFTEN - ECSA E.V.	Germany
9	FRAUNHOFER GESELLSCHAFT ZUR FOERDERUNG DER ANGEWANDTEN FORSCHUNG E.V.	Germany
10	STICHTING IMEC NEDERLAND	Netherlands
11	ASSOTSIATSIA ZA RAZVITIE NA SOFIA	Bulgaria
12	SODAQ HOLDING BV	Netherlands
13	REAR WINDOW	Belgium
14	PANEPISTIMIO AIGAIOU	Greece
15	VLAAMSE MILIEUMAATSCHAPPIJ	Belgium

4. Project contact details

Coordinator	Technical Specialists
Lieven Raes lieven.raes@vlaanderen.be	Project Manager: Marina Klitsi (m.klitsi@atc.gr) Technical Manager: Sakis Dalianis (T.Dalianis@atc.gr)

II. ABOUT THE RESEARCH PARTICIPANT

In the event you would like to participate in the Research, please provide us with the following information, which will be processed in accordance with the below Privacy Policy:

First name _____

Last name _____

Email address _____

III. RESEARCH CONSENT

I volunteer to participate in the Research described above conducted in the context of the COMPAIR Project.	Yes	No
I understand that my participation is voluntary (my choice).	Yes	No
I understand that I will not receive any financial compensation for my participation.	Yes	No
I am aware that I have the right to withdraw from the Research at any time in the Project.	Yes	No
I have read and understood the explanation provided to me about the Project.	Yes	No
I have read and understood the Privacy Policy and I understand that my personal data will be processed as described in the Privacy Policy.	Yes	No
I agree to have my role and/or organisation mentioned in the reports, including public reports, to be submitted to the European Commission and published online.	Yes	No
I have had all my questions answered to my satisfaction.	Yes	No
I know who to contact if I have any question about the Project and my privacy.	Yes	No
I have been given a copy of this participation form.	Yes	No

First name _____

Last name _____

Signature _____

Date _____ City / Town _____

IV. PRIVACY POLICY

1. Scope of this policy

This Privacy Policy describes how your personal data is collected, used and otherwise processed in the context of the EU COMPAIR Project funded under the H2020 research programme, contract no. H2020-101036563 (hereafter the "**Project**").

This Privacy Policy includes a description of your data protection rights, including a right to object to some of the processing activities we carry out.

In this Privacy Policy:

- "**We**" or "**us**" refer to the Partners of the COMPAIR Project listed in Section I.3. above, who will process your personal data as data controllers and as described herein.
- "**Data Protection Legislation**" means the Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the "**GDPR**"), as well as any legislation and/or regulation implemented or created pursuant to the GDPR and the e-Privacy legislation, or which amends, replaces, re-enacts or consolidates any of them, and all other national applicable laws relating to processing of personal data and privacy that may exist under applicable law.
- The terms "controller", "processor", "third party", "supervisory authority", "personal data", "processing", "data subject", shall have the meanings set out in the applicable Data Protection Legislation.

2. What personal data is processed?

In the context of the Project, your personal data is processed by the Plovdiv Partners, as follows:

- **Processing purpose(s):** for the purpose of carrying out the research in the COMPAIR Project, as described in Section I above.
- **Processed data categories:** first name, last name, email address, age, school.
- **Source of data:** from the participant, directly.
- **Legal basis:** Our legitimate interests. It is in the Partners' legitimate interests to process your personal data as a Research participant. We will always make sure that your interests are safeguarded. This does not affect your rights, as described below.

3. How long is your personal data stored?

We retain your personal data for as long as is required to fulfil the activities set out in the Participation Form and this Privacy Policy, for as long as otherwise communicated to you or for as long as is permitted by applicable law. For example, we may retain your personal data if it is reasonably necessary to comply with any legal obligations, meet any regulatory requirements, resolve any disputes or litigation, or as otherwise needed to enforce this

Privacy Policy and prevent fraud and abuse. This period will last until October 2024, by the end of the project.

4. **How is your personal data shared with third parties?**

The data that we collect from you as described in this Privacy Policy will not be shared with any third parties.

5. **Is your personal data transferred outside the European Economic Area (EEA)?**

The data that we collect from you as described in this Privacy Policy will not be transferred to and stored at a destination outside the EEA.

6. **What are your rights?**

Once you have provided your personal data, several rights are recognized under the Data Protection Legislation, which you can in principle exercise free of charge, subject to statutory exceptions. In particular, you have the following rights:

- **Right to access, review, and rectify your data:** you have the right to access, review, and rectify your personal data. You may be entitled to ask us for a copy of your information, to review or correct it if you wish to review or rectify any information. You may also request a copy of the personal data processed as described herein by sending an email to ethics@wecompair.eu. You can access and review this information and, if necessary, ask to rectify your information.
- **Right to erasure:** you have the right to erasure of all the personal data processed by as described herein in case it is no longer needed for the purposes for which the personal data was initially collected or processed, in accordance with the Data Protection Legislation.
- **Right to object or restriction of processing:** under certain circumstances described in the Data Protection Legislation, you may ask for a restriction of processing or object to the processing of your personal data.
- **Right to data portability**: you have the right to receive the Personal Data processed in a format which is structured, commonly used and machine-readable and to transmit this data to another service provider.

These rights may be limited, for example if fulfilling your request would reveal personal data about another person, or if you ask us to delete information which we are required by law to keep or have compelling legitimate interests in keeping.
To exercise any of these rights, you can get in touch with us using the details set out below. If you have unresolved concerns, you have the right to lodge a complaint with an EU data protection authority where you live, work or where you believe a breach may have occurred.

7. **What security measures are put in place?**

Appropriate technical and organisational measures are implemented in order to ensure an appropriate level of security of your personal data.
In the event personal information is compromised as a result of a security breach and where the breach is likely to result in a high risk to your rights and freedoms, we will make the necessary notifications, as required under the Data Protection Legislation.

8. **How can we be contacted?**

Questions, comments, remarks, requests or complaints regarding this Privacy Policy are welcome and should be addressed to ethics@wecompair.eu.

Sofia Consent Form

PARTICIPATION FORM & PRIVACY POLICY

I. ABOUT THE RESEARCH PROJECT

1. COMPAIR EU-funded Project

COMPAIR is an EU Innovation Action (IA) project. Its main focus will be on bolstering citizens' capacity to monitor, understand, and change their environmental impact, both at a behavioural and policy level. It unlocks the power of the wider public, including people from lower-socio economic groups, to provide broad granular data around a central theme of air quality, complementing and improving the quality of official datasets and making new information useful for research purposes, policy making and behavioural change.
The COMPAIR project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101036563. The COMPAIR project started on 1 November 2021 and has a duration of 36 months.

2. Research aspects

The Sofia pilot in the COMPAIR project aims to investigate the traffic and solid fuel domestic heating in order to reduce the corresponding levels and, thus, to improve air quality. These goals will be materialised via two use cases. The first one focuses on testing ambient air quality indoors and outdoors in one of the biggest kindergartens in Sofia and aims to evaluate the efficiency of window meshes at reducing indoor PM levels. The second one focuses on testing school bus pilot service and how it affects traffic and air quality around schools in order to determine the impact of the introduction of school bus routes for morning and noon transport to school.

3. Project Partners

The partners of the COMPAIR project are the following:

	Organisation Name	Country
1	VLAAMSE GEWEST (Project coordinator)	Belgium
2	IS-PRACTICE BVBA	Belgium
3	ATHENS TECHNOLOGY CENTER ANONYMI VIOMICHANIKI EMPORIKI KAI TECHNIKI ETAIREIA EFARMOGON YPSILIS TECHNOLOGIAS	Greece
4	INTER 3 GMBH INSTITUT FUR RESSOURCENMANAGEMENT	Germany
5	21C CONSULTANCY LIMITED	United Kingdom
6	DIMOS ATHINAION EPICHEIRISI MICHANOGRAFISIS	Greece
7	ENERGY AGENCY OF PLOVDIV ASSOCIATION	Bulgaria

8	VEREIN DER EUROPAEISCHEN BURGERWISSENSCHAFTEN - ECSA E.V.	Germany
9	FRAUNHOFER GESELLSCHAFT ZUR FOERDERUNG DER ANGEWANDTEN FORSCHUNG E.V.	Germany
10	STICHTING IMEC NEDERLAND	Netherlands
11	ASSOTSIATSIA ZA RAZVITIE NA SOFIA	Bulgaria
12	SODAQ HOLDING BV	Netherlands
13	REAR WINDOW	Belgium
14	PANEPISTIMIO AIGAIOU	Greece
15	VLAAMSE MILIEUMAATSCHAPPIJ	Belgium

4. Project contact details

Coordinator	Technical Specialists
Lieven Raes lieven.raes@vlaanderen.be	Project Manager: Marina Klitsi (m.klitsi@atc.gr) Technical Manager: Sakis Dalianis (T.Dalianis@atc.gr)

II. ABOUT THE RESEARCH PARTICIPANT

In the event you would like to participate in the Research, please provide us with the following information, which will be processed in accordance with the below Privacy Policy:

First name _____

Last name _____

Email address _____

III. RESEARCH CONSENT

I volunteer to participate in the Research described above conducted in the context of the COMPAIR Project.	Yes	No
I understand that my participation is voluntary (my choice).	Yes	No
I understand that I will not receive any financial compensation for my participation.	Yes	No
I am aware that I have the right to withdraw from the Research at any time in the Project.	Yes	No
I have read and understood the explanation provided to me about the Project.	Yes	No
I have read and understood the Privacy Policy and I understand that my personal data will be processed as described in the Privacy Policy.	Yes	No
I agree to have my role and/or organisation mentioned in the reports, including public reports, to be submitted to the European Commission and published online.	Yes	No
I have had all my questions answered to my satisfaction.	Yes	No
I know who to contact if I have any question about the Project and my privacy.	Yes	No
I have been given a copy of this participation form.	Yes	No

First name _____

Last name _____

Signature _____

Date _____ City / Town

_____

IV. PRIVACY POLICY

1. Scope of this policy

This Privacy Policy describes how your personal data is collected, used and otherwise processed in the context of the EU COMPAIR Project funded under the H2020 research programme, contract no. H2020-101036563 (hereafter the "**Project**").

This Privacy Policy includes a description of your data protection rights, including a right to object to some of the processing activities we carry out.

In this Privacy Policy:

- "**We**" or "**us**" refer to the Partners of the COMPAIR Project listed in Section I.3. above, who will process your personal data as data controllers and as described herein.
- "**Data Protection Legislation**" means the Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the "**GDPR**"), as well as any legislation and/or regulation implemented or created pursuant to the GDPR and the e-Privacy legislation, or which amends, replaces, re-enacts or consolidates any of them, and all other national applicable laws relating to processing of personal data and privacy that may exist under applicable law.
- The terms "controller", "processor", "third party", "supervisory authority", "personal data", "processing", "data subject", shall have the meanings set out in the applicable Data Protection Legislation.

2. What personal data is processed?

In the context of the Project, your personal data is processed by the Sofia Partners, as follows:

- **Processing purpose(s):** for the purpose of carrying out the research in the COMPAIR Project, as described in Section I above.
- **Processed data categories:** first name, last name, email address, place of study (school), school grade, IP address.
- **Source of data:** from the participant, directly.
- **Legal basis:** Our legitimate interests. It is in the Partners' legitimate interests to process your personal data as a Research participant. We will always make sure that your interests are safeguarded. This does not affect your rights, as described below.

We rely on the following organisations to process your personal data:

Organisation	Processed data categories	Instructions

(data processor)		
Google Forms	first name, last name, email address, place of study (school), school grade, IP address (where applicable)	Provision of survey tool allowing for the creation and sending of Research questionnaires.
MS Office Forms	first name, last name, email address, place of study (school), school grade, IP address (where applicable)	Provision of survey tool allowing for the creation and sending of Research questionnaires.

3. How long is your personal data stored?

We retain your personal data for as long as is required to fulfil the activities set out in the Participation Form and this Privacy Policy, for as long as otherwise communicated to you or for as long as is permitted by applicable law. For example, we may retain your personal data if it is reasonably necessary to comply with any legal obligations, meet any regulatory requirements, resolve any disputes or litigation, or as otherwise needed to enforce this Privacy Policy and prevent fraud and abuse. This period will last until October 2024, by the end of the project.

4. How is your personal data shared with third parties?

The data that we collect from you as described in this Privacy Policy will not be shared with any third parties.

5. Is your personal data transferred outside the European Economic Area (EEA)?

The data that we collect from you as described in this Privacy Policy will not be transferred to and stored at a destination outside the EEA.

6. What are your rights?

Once you have provided your personal data, several rights are recognized under the Data Protection Legislation, which you can in principle exercise free of charge, subject to statutory exceptions. In particular, you have the following rights:

- **Right to access, review, and rectify your data:** you have the right to access, review, and rectify your personal data. You may be entitled to ask us for a copy of your information, to review or correct it if you wish to review or rectify any information. You may also request a copy of the personal data processed as described herein by sending an email to ethics@wecompair.eu. You can access and review this information and, if necessary, ask to rectify your information.
- **Right to erasure:** you have the right to erasure of all the personal data processed by as described herein in case it is no longer needed for the purposes for which the personal data was initially collected or processed, in accordance with the Data Protection Legislation.
- **Right to object or restriction of processing:** under certain circumstances described in the Data Protection Legislation, you may ask for a restriction of processing or object to the processing of your personal data.

- **Right to data portability**: you have the right to receive the Personal Data processed in a format which is structured, commonly used and machine-readable and to transmit this data to another service provider.

These rights may be limited, for example if fulfilling your request would reveal personal data about another person, or if you ask us to delete information which we are required by law to keep or have compelling legitimate interests in keeping.
To exercise any of these rights, you can get in touch with us using the details set out below. If you have unresolved concerns, you have the right to lodge a complaint with an EU data protection authority where you live, work or where you believe a breach may have occurred.

7. What security measures are put in place?

Appropriate technical and organisational measures are implemented in order to ensure an appropriate level of security of your personal data.
In the event personal information is compromised as a result of a security breach and where the breach is likely to result in a high risk to your rights and freedoms, we will make the necessary notifications, as required under the Data Protection Legislation.

8. How can we be contacted?

Questions, comments, remarks, requests or complaints regarding this Privacy Policy are welcome and should be addressed to ethics@wecompair.eu.