Ref. Ares(2022)718121 - 31/01/2022

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement n° 101037648 – SOCIO-BEE

Socio Bee

Grant Agreement No: 101037648
[H2020-LC-GD-2020-3]

Wearables and droneS fOr CIty Socio-Environmental Observations and Behavioral ChangE

Deliverable

D3.1. – Report on Legal and Regulatory Requirements

Workpackage No.	**WP3**	Workpackage Title	**SOCIO-BEE platform requirements definition and analysis**
Task No.	**T3.1**	Task Title	**Legal and Regulatory Requirements**
Lead beneficiary		**VUB (LSTS)**	
Dissemination level		**PU**	
Nature of Deliverable		**R**	
Delivery date		**31 January 2022**	
Status		**D**	
File Name:		**[SocioBee] D3.1 – Report on Legal and Regulatory Requirements_v1.8.docx**	
Project start date, duration		**01 October 2021, 36 Months**	

Authors List

Leading Author (Editor)				
Surname		*Initials*	*Beneficiary Name*	*Contact email*
van der Veer		LVDV	VUB	Luka.van.der.veer@vub.be
Gkotsopoulou		OG	VUB	Olga.gkotsopoulou@vub.be
Quinn		PQ	VUB	Paul.quinn@vub.be
Co-authors (in alphabetic order)				
#	*Surname*	*Initials*	*Beneficiary Name*	*Contact email*
1	Ververidis	CV	HYP	c.ververidis@hypertech.gr
2	Tsiakoumi	MT	HYP	desk@hypertech.gr
3	Amadei	CA	UNIPD	claudia.amadei@unipd.it
4	Ramirez	FR	BETTAIR	framirez@bettaircities.com
5	Karanasos	DK	CERTH	dkaranassos@iti.gr
6	Drosou	AD	CERTH	drosou@iti.gr
7	Doran	CD	ECSA	Carolina.Doran@mfn.berlin

Reviewers List

List of Reviewers (in alphabetic order)				
#	*Surname*	*Initials*	*Beneficiary Name*	*Contact email*
1	*Kopsacheilis*	*EK*	*CERTH*	*Ekops@iti.gr*
2	*Grigoriadis*	*DG*	*HYP*	*d.grigoriadis@hypertech.gr*

Document History			
Date	*Version*	*Author*	*Description*
3/12/2021	1.1	**VUB**	Prepared ToC – internal review
17/01/2022	1.2	**ECSA**	Input chapter 2: Citizen Science – comments and paragraph
17/01/2022	1.3	**UNIPD**	Input chapter 2: Citizen Science – comments and paragraph
18/01/2022	1.4	**HYP & CERTH**	Input chapter 3: Drones and 5: Machine Learning and AI – comments and paragraphs
19/01/2022	1.5	**AUTH**	Input Chapter 5: Machine Learning and AI – paragraph on definition SOCIO-BEE
21/01/2022	1.6	**BETTAIR**	Input Chapter 4: Wearables – parapraph on future developments of technologies
28/01/2022	1.7	**HYP & CERTH**	Feedback from Peer Review
28/01/2022	1.8	**VUB**	Internal feedback

List of abbreviations

Abbreviation	Description
AI	Artificial Intelligence
CAHAI	Ad hoc Committee on Artificial Intelligence
CJEU	Court of Justice of the European Union
CoE	Council of Europe
DPA	Data Protection Authority
EASA	European Union Aviation Safety Agency
EC	European Commission
ECHR	European Convention on Human Rights
ECSA	European Citizen Science Association
ENISA	European Union Agency for Cybersecurity
EU	European Union
ESC	European Social Charter
FDA	Food and Drug Authorities

GDPR	General Data Protection Regulation
ICAO	International Civil Aviation Organisation
ML	Machine Learning
RPAS	Remotely Piloted Aircraft Systems
TFEU	Treaty on the Functioning of the European Union
UAV	Unmanned aerial vehicle
UN	United Nations
UK	United Kingdom
USA	United States of America

Table of Contents

Table of Figures

List of Tables

Executive Summary

Deliverable 3.1 is the first deliverable of the WP3 and reports on the baseline legal and regulatory requirements relevant for the SOCIO-BEE context. The report builds upon four main pillars that discuss the most important and relevant legal and regulatory frameworks of:

Citizen science and Air pollution: legal and regulatory framework

Citizen science is a popular phenomenon that has various definitions. An important feature, however, is that citizens participate in data collection for scientific research. Its relation to some important developments in the field of European fundamental rights on air pollution and science and the role of data in citizen science and European environmental policy are important topics of discussion within the international and European context and are relevant to the deliverable.

Use of drones in Socio Bee context: legal and regulatory framework

From 31 December 2020, the new European regulatory framework for drones applies to all existing and future drone activities. This framework, based on *Regulations (EU) 2019/947 and 2019/945,* will ensure the safe operation of civilian drones in European airspace, as well as facilitate the development of innovative applications and the creation of a European market for unmanned aerial services. It will also facilitate the enforcement of citizens' privacy rights and help address security and environmental concerns for the benefit of EU citizens. An essential element in this framework is that they do not distinguish between recreational or commercial civil drone activities by adopting a risk-based approach. The European Regulation also provide some flexibility for the member states to develop acts to define certain aspects.

Use of wearables in Socio Bee context: legal and regulatory framework

The use of wearables will only increase in the coming years in different areas. Since these devices are connected a part of the Internet of Things, it is necessary to consider both components. The biggest challenge for the project is to secure wearables against cyberattacks and surveillance. The EU has already developed several strategies and legislative frameworks to address this such as the Cybersecurity Act and Cybersecurity Strategy 2020.

Use of artificial intelligence and machine learning in Socio Bee context: legal and regulatory framework

Regulatory and legislative frameworks have only recently been developed and because technology is constantly evolving at a rapid pace, it remains a challenge to capture all these recent developments. There are no international or European legal instruments specifically addressing the challenges of AI systems to human rights in a comprehensive manner at the moment. In the EU many initiatives and approaches have emerged over the years to accommodate these concerns, becoming a central policy question in the EU that are relevant for the coming years. That is why the European Commission has proposed a new AI Act, which is currently being drafted.

1 Introduction

1.1 Project overview

SOCIO-BEE proposes that community engagement and social innovation combined with Citizen Science (CS) through emerging technologies and playful interaction can bridge the gap between 1) the capacity of communities to adopt more sustainable behaviours, breaking the cognitive myopia, and 2) between the citizen intentions and the real behaviour to act in favour of the environment (in this project, to reduce air pollution). Furthermore, community engagement can raise other citizens' awareness of climate change and their own responses to it, through experimentation, better monitoring, and observation of the environment. This idea is emphasised in this project through the metaphor of bees' behaviour (with queens, worker and drone bees), interested stakeholders (honey bears) and the Citizen Science hives that will be tested in three different pilot sites and with different population: young adults, elderly people and everyday commuters.[1]

1.2 Purpose of the document

Task 3.1 and specifically D3.1 will explore, map and scrutinize the applicable legal and regulatory framework, taking into consideration the particularities of citizen science research. Specifically, in it, the SOCIO-BEE consortium will focus upon the study of three umbrella frameworks, namely: a) the relevant international and European fundamental rights framework, b) the relevant European Union framework and c) the respective national framework. The study of those frameworks will be complemented by taking into consideration case law and other non-binding guidance issued by competent authorities. Furthermore, this task will present not only in force legal and regulatory frameworks, but additionally emerging or developing legislation, regulation and policy which may have an impact on the future implementation of the SOCIO-BEE platform, allowing the key decision makers of the consortium to make informed decisions in relation to platform sustainability. This report is a follow up to the informative workshop that took place in the kick-off meeting off the project, organized by VUB-LSTS and will include a concise overview of the applicable framework, a first set of high-level recommendations and an operational legal glossary, enhancing cross-disciplinary cooperation, at an early stage of the project.[2]

1.3 Relationship with other deliverables

D3.1 is closely related to D1.5 and all the deliverables of WP6, providing a baseline for further research.

1.4 Structure of document

The division of this deliverable is built around discussing the respective legal and regulatory frameworks applicable for the SOCIO-BEE project. These are: Citizen science and Air pollution; the use of drones; the use of wearables; the use of Artificial Intelligence and Machine Learning.

Each time the context is outlined on an international level, to be followed by a more in-depth discussion on the European context and possibly also national legal and regulatory frameworks where relevant. Also, where applicable, future developments are discussed so that the consortium is aware of the possible implications of new developments in the coming years. Because of the participation of vulnerable groups

[1] Call: H2020-LC-GD-2020: SOCIO-BEE, GA No: 101037648, p. 2
[2] Ibid., p. 50

such as the elderly and children, additional information is provided in each section where possible. Finally, attention is given to possible challenges and each section concludes with preliminary recommendations.

2 Citizen science and Air pollution: Legal and regulatory framework

2.1 What is Citizen Science

2.2 No commonly agreed definition, despite the long history

In literature, there are numerous definitions of citizen science (CS). A crucial point is the voluntary participation of citizens. Most definitions describe CS "as a form of science in which the general public contributes to the production of scientific knowledge, either alone or more often in cooperation with professional scientists and scientific institutions". However, not all these participations would fall under the definition of CS, given that the minimum standards for citizen science vary in the literature and among projects and organisations.

The participation of citizens in science has a long history. The involvement of citizens in scientific work is not something new and exclusive to the 21st century. The history of science makes it clear that lay expertise and assistance almost always occupied an important position within science in societies in which it unfolded. Famous examples include the great natural history observations such as those of Charles Darwin and Wallace.[3] In any case, there is no consensus from the academic literature and within the citizen science community as to what citizen science exactly entails.

2.2.1 The layered definition of Citizen Science: bottom-up and top-down

Within the academic community, CS has two fundamentally different origins in the 1990s. The two are also distinguished from each other by using the dichotomy *bottom-up* and *top-down citizen science*. In bottom-up citizen science the focus is on the grassroots character, where citizens themselves engage in citizen science to address a problem or produce new knowledge. These initiatives are linked to the work of Irwin (1995). Top-down, on the other hand, refers to the fact that the project is directed or initiated from above by scientists / institutions. These initiatives are linked to the work of Bonney (1996).

A recent review shows that these two terms are not as far apart as thought. Although the majority of literature and projects focus on Bonney's framework (i.e. that of participation in science), it is hypothesised that the general popularity for citizen science projects may pave the way for a more democratic version of science in society. For example, they note that "more and more practitioners of citizen science (any kind) see the democratic, more activist citizen science along the lines of Irwin's (1995) idea as “the end goal".

This is especially apparent in projects involved in environmental issues. Over the years, many typologies have emerged to classify citizen science projects and to better understand the concept. The most important lesson is that citizen science can have different types of initiatives depending on the role assigned to the citizen. For example, the citizen could only participate in data collection, but can also expand and move towards analysing data and finding conclusions.[4]

The majority of citizen science projects are ‘contributory’, i.e. designed by academics/research organisations, but entailing the collection of monitoring data by volunteers. However, initiatives with greater public involvement in the scientific process have recently been on the rise, i.e. ‘collaborative’ projects (designed by researchers, with volunteers contributing data, refining project design, analysing

[3] A whole network of volunteers participated in observing, classifying and collecting data on nature.

[4] A well-known work that breaks down these different types is the work of Arnstein’s Ladder of Citizen Participation (1969). In it, she sets up a participation ladder that divides the role of citizens in participating in policy which later also influenced citizens' participation in scientific research.

data and/or disseminating findings) and 'co-created' initiatives (volunteers and researchers work together throughout).[5]

2.2.2 The urge for standardization in Citizen Science

There are several calls in the academic literature and in practice to introduce some more standardisation within the diversity of definitions, methods and practices that constitute CS so that high quality participatory research is ensured.[6] By having a minimum set of criteria that ensure scientifically correct data and methods, it would reduce the reluctance of policy makers to base their decision making on data collected through CS initiatives. If not, policymakers may be afraid that the data and results will not be taken seriously because they cannot guarantee their reliability.

Standardisation can also help when seeking funding for a project so that agencies have a better idea of what to expect from the project. However, it is also noted that these attempts at further definition may come at the expense of some of the possible characteristics of CS, such as its openness and capacity for creativity and innovative methodology. A common important reference to a general definition are: *The 10 Principles of Citizen Science* compiled by the European Citizen Science Association.[7] These 10 principles are a summary of best practices that projects can meaningfully engage with. The principles are as below:

1. *Citizen science projects actively involve citizens in scientific endeavour that generates new knowledge or understanding. Citizens may act as contributors, collaborators, or as project leader and have a meaningful role in the project.*
2. *Citizen science projects have a genuine science outcome. For example, answering a research question or informing conservation action, management decisions or environmental policy.*
3. *Both the professional scientists and the citizen scientists benefit from taking part. Benefits may include the publication of research outputs, learning opportunities, personal enjoyment, social benefits, satisfaction through contributing to scientific evidence e.g. to address local, national and international issues, and through that, the potential to influence policy.*
4. *Citizen scientists may, if they wish, participate in multiple stages of the scientific process. This may include developing the research question, designing the method, gathering and analysing data, and communicating the results.*
5. *Citizen scientists receive feedback from the project. For example, how their data are being used and what the research, policy or societal outcomes are.*

[5] European Commission, COMMISSION STAFF WORKING DOCUMENT, Best Practices in Citizen Science for Environmental Monitoring, SWD(2020) 149 final, p. 7 - 8

[6] Heigl, F., Kieslinger, B., Paul, K.T., Uhlik, J., & Dörler, D. (2019). Toward an international definition of citizen science. *PNAS*, 116(17), 8089-8092. doi:10.1073/pnas.1903393116

[7] ECSA, 'ECSA's characteristics of citizen science'. (April 2020). Available : https://ecsa.citizen-science.net/wp-content/uploads/2020/05/ecsa_characteristics_of_citizen_science_-_v1_final.pdf

6. *Citizen science is considered a research approach like any other, with limitations and biases that should be considered and controlled for. However unlike traditional research approaches, citizen science provides opportunity for greater public engagement and democratisation of science.*
7. *Citizen science project data and meta-data are made publicly available and where possible, results are published in an open access format. Data sharing may occur during or after the project, unless there are security or privacy concerns that prevent this.*
8. *Citizen scientists are acknowledged in project results and publications.*
9. *Citizen science programmes are evaluated for their scientific output, data quality, participant experience and wider societal or policy impact.*
10. *The leaders of citizen science projects take into consideration legal and ethical issues surrounding copyright, intellectual property, data sharing agreements, confidentiality, attribution, and the environmental impact of any activities.*

However, as recognized in preamble of the document by ECSA that contains the principles, this is only one of the many interpretations of the flexible concept of citizen science. Finally, the value of citizen science has been widely recognised in the literature and in practice. Among other things, it has value for policy, science and society in general.

2.3 Citizen science as defined in SOCIO-BEE

A key goal in SOCIO-BEE is to empower people to pay more attention to how their behaviours impact the environment and make long lasting changes accordingly. In order to achieve this, the SOCIO-BEE consortium is currently developing an engagement strategy (WP2) which at its core, focusses on meaningful engagement of individuals with different levels of commitment to improving air quality. With the planned pilots, the consortium aims to include citizen scientists from the beginning of the process by learning from them what are their concerns and what barriers they face and work together towards fixing those. For its definition, the project will follow guidelines by ECSA and the 10 Principles of Citizen Science as seen earlier.[8]

2.4 The international framework

The work, debates and development of CS are also closely associated with the Sustainable Development Goals (SDGs) of the United Nations (UN).[9] The work of Citizen Science Global Partnership and the European Citizen Science Association (ECSA) will ensure that CS is promoted and discussed in relation to these SDGs.[10] It mainly looks at the different ways in which volunteer-generated data could contribute to the SDG indicator framework. “Following the participation of citizen science delegations in the third and

[8] ECSA, ‘ECSA’s characteristics of citizen science’. (April 2020). Available : https://ecsa.citizen-science.net/wp-content/uploads/2020/05/ecsa_characteristics_of_citizen_science_-_v1_final.pdf
[9] The Sustainable Development Goals are objectives that member states of the United Nations to work towards sustainable development by 2030. [Online]. Available: https://sdgs.un.org/goals
[10] http://citizenscienceglobal.org/projects.html#his

fourth (2018 and 2019) meetings of the UN Science-Policy-Business Forum on the Environment[11], these potential contributions have clearly been recognized".[12] [13] [14]

In 2017 several initiatives were worldwide launched to carry work that is needed as part of the SDGs.[15] These international developments are therefore evidence of a recognition of the value and potential of CS. This includes its contribution to data collection, data collection methodologies, indicator development and assessment.

Specifically in the context of the SDGs, these activities have additional social and economic impacts, and also address issues of environmental policy – which is relevant to the SOCIO-BEE project.[16] Examples of networks for the integration of CS into policies at international (global) level constitute:

- Citizen Science Global Partnership[17]
- Citizen Cyberlab[18]

Additionally, more CS institutions, associations, networks have emerged worldwide. Further examples include:

- US Citizen Science Association (CSA)[19]
- US Environmental Protection Agency (EPA), which has published several strategic documents on citizen science, including a vision for citizen science at EPA and a Handbook for citizen science quality assurance and documentation[20]
- Australian Citizen Science Association (ACSA)[21]
- Citizen Science Asia[22]
- African Citizen Science Association[23]

2.4.1 A right to science?

2.4.1.1 Science and the public

The popularity of the concept is therefore not without consequences as it possibly points to "a potential transformation in the modes of public participation in science".[24] Indeed, the concept is located in a longer history of public participation in science and has the potential to challenge the authority of institutionalised science. It thus relates to the established relationship between professional scientists (in

[11] https://citizenscience.org.au/2019/02/11/citizen-science-on-the-world-stage-at-unea4-in-nairobi/
[12] http://web.unep.org/environmentassembly/major-groups-and-stakeholder-science-and-technology;
[13] https://www.unep.org/environmentassembly/
[14] European Commission, COMMISSION STAFF WORKING DOCUMENT, Best Practices in Citizen Science for Environmental Monitoring, SWD(2020) 149 final, p. 14
[15] https://mediamanager.sei.org/documents/Publications/SEI-2017-PB-citizen-science-sdgs.pdf. Ibid., p. 14 These initiatives include helping the citizen science community see how it can contribute to the SDG framework, support for data management and a focus on citizen science contributions relating to Earth observation data and tools.
[16] European Commission, COMMISSION STAFF WORKING DOCUMENT, Best Practices in Citizen Science for Environmental Monitoring, SWD(2020) 149 final, p. 14
[17] http://citizenscienceglobal.org/
[18] http://citizencyberlab.org/
[19] https://www.citizenscience.org/
[20] https://www.epa.gov/citizen-science
[21] https://citizenscience.org.au/
[22] https://www.facebook.com/CitSciAsia
[23] https://techmoran.com/2017/12/07/usiu-africa-to-host-the-first-african-citizen-science-association/
[24] Strasser, B. J., Baudry, J., Mahr, D., Sanchez, G. and Tancoigne, E. (2019) 'Citizen Science'? Rethinking Science and Public Participation, *Science & Technology Studies*, *32*(2), p. 52–76. doi:10.23987/sts.60425, p. 52

research institutions) and the public in which it is assumed that scientists produce scientific knowledge and the public primarily consumes science and technology.[25] This relationship has been at odds throughout the 20th century. Citizen science could therefore bring about profound transformations such as a better understanding of science or a more democratic science and thus reduce or reinforce this tension.[26]

2.4.1.2 The question of trust

From the 1980s onwards, there was increasing talk of a crisis of trust between the public and science. In response to this, various institutional experimentations by governments and international organisations arose in order to restore this trust, with participation becoming an important key word in solving the trust problem.[27] The literature speaks more generally of the participatory turn, which promoted various forms of public participation in science and technology.

This turn was based on a deliberative democracy that involved citizens in the decision-making or formulation of science policy, research agendas and (the implementation of) technological choices, thus giving the public a voice in debates about which issues or research were of general interest. This, however, was seen as a way to regain trust in public authorities and policy in a more general sense. As a result, these developments are reflected at both international and European level.

The bottom-up work of Irwin[28] also shows with a variety of cases that knowledge produced by non-experts/learners must be recognised. This applies to his research in the fields of environmental and health policy, which in turn are linked to scientific-technological development.

For example, citizen science is currently included as part of the Responsible Research & Innovation (RRI) of the EU programme Horizon 2020. Involving citizens at an early stage in the Research & Development process can be facilitated by citizen science.[29] This will be discussed further in the chapter on Europe.

2.4.1.3 A fundamental right to (the participation of) science

From the framework of UN human rights, the right to science emerged as "the right to share in scientific progress and its benefits"[30] and then later in the framework of social and cultural rights. [31] Specifically, the right to science is provided in Article 27 of the Universal Declaration of Human Rights:

> (1) *Everyone has the right freely to participate in the cultural life of the community, to enjoy the arts and to share in scientific advancement and its benefits.*

[25] Strasser, B. J., Baudry, J., Mahr, D., Sanchez, G. and Tancoigne, E. (2019) 'Citizen Science'? Rethinking Science and Public Participation, *Science & Technology Studies*, *32*(2), p. 52–76. doi:10.23987/sts.60425; Hecker, S., Haklay, M., Bowser, A., & Makuch, Z. (2018). *Citizen Science: Innovation in Open Science, Society and Policy*. London: UCL Press.

[26] This extract is based on my thesis. See: van der Veer, L. (2020). *Op weg naar een democratisering van wetenschappelijk onderzoek? Een studie naar de verschillende gedaantes van Citizen Science in Vlaanderen* (Master's thesis, KU Leuven, Leuven, Belgium). [Dutch]

[27] Chilvers, J., & Kearnes, M. (2020). Remaking Participation in Science and Democracy. Science, Technology, & Human Values, *45*(3), p. 347–380. doi:10.1177/0162243919850885

[28] Irwin, A. (1995). *Citizen Science: A Study of People, Expertise, and Sustainable Development. Environment and Society*. London: Routledge.

[29] This is also seen as a test case for open science, "the most interesting way to democratise science". See Gijsel, L., Huye, T., & Van Hoyweghen, I. (2019). *Citizen science: hoe burgers de wetenschap uitdagen*. Kalmthout: Pelckmans Pro. [Dutch]

[30] Art. 27 in UN 1948; UN (United Nations). (1948). Universal declaration of human rights. https://www.un.org/en/universal-declaration-human-rights/

[31] Art. 15 in UN 1966; UN (United Nations). (1966). International covenant on economic, social and cultural rights. https://www.ohchr.org/en/professionalinterest/pages/cescr.aspx

> (2) *Everyone has the right to the protection of the moral and material interests resulting from any scientific, literary or artistic production of which he is the author.*

The right to science is also envisaged in Article 15 of the International Covenant on Economic, Social and Cultural Rights:

> *[…]*
>
> *(b) To enjoy the benefits of scientific progress and its applications;*
>
> *(c) To benefit from the protection of the moral and material interests resulting from any scientific, literary or artistic production of which he is the author.*
>
> *[…]*
>
> *(3) The States Parties to the present Covenant undertake to respect the freedom indispensable for scientific research and creative activity.*

The meaning of this changed over the last two decades from "the right to access information and knowledge, as well as the benefits of different scientific and technological developments" to the right to participate. [32] [33] This was mainly due to decision making on risks in environmental and health issues. Increasingly, citizens would be actively involved in the research itself, which would shift the interpretation to 'just' a "right to participate". The aforementioned SDGs are a good example of an increasingly actively involved public in sustainable development. For example, the 'right to participate in environmental decision-making' was recognised by the United Nations Economic Commission for Europe in 1998. This came about with the adoption of the Aarhus Convention.[34]

This right was recently mentioned for the first time in an official UN publication.[35] In it, the Special Rapporteur for the UN to the UN Human Rights Council framed this right as "the right to enjoy the benefits of scientific progress and its applications". Particularly timely for the present research is part (b) of Shaheed's reasoning, where she defines the right as entailing the 'opportunities for all to contribute to the scientific enterprise and freedom indispensable for scientific research' and part (c) where she envisages for 'participation of individuals and communities in decision-making and the related right to information".[36] [37] This was an important starting point for further discussions on the conceptual interpretation and practical application of this right. In the long term, official recognition of this right may be applicable, which will also lead to further guidance for different stakeholders and institutions.[38] As

[32] Schade et al. (2021). Chapter 18 – Citizen Science and Policy. In K., Vohland, A., L.and-Zandstra., L., Ceccaroni, R., Lemmens, J., Perelló, M., Ponti, R., Samson, & K., Wagenknecht (Eds.). *The Science of Citizen Science.* (pp. 357) New York: Springer.

[33] De Marchi, B., Funtowicz, S., & Guimarães-Pereira, A. (2001). From the right to be informed to the right to participate: Responding to the evolution of European legislation with ICT. *International Journal of Environment and Pollution*, 15(1), 1–21.

[34] 1998 Aarhus Convention on Access to Information, Public Participation in Decision-Making and Access to Justice in Environmental Matters

[35] Farida Shaheed, 'The right to enjoy the benefits of scientific progress and its applications' (A/HRC/20/26, HRC 2012).

[36] Ibid.

[37] Berti Suman, A., & Pierce, R. (2018). Challenges for citizen science and the EU open science agenda under the GDPR. *European Data Protection Law Review,* 4(3), 284-295. doi10.21552/edpl/2018/3/7

[38] Audrey Chapman and Jessica Wyndham, 'A Human Right to Science' (2013) 340(6138) Science

such, CS could be seen as a rightful practice in itself in the nearby future that is based on a right the science.[39]

2.5 The European framework

When we speak about the European framework, we refer both to the European Union and the Council of Europe framework. Those two frameworks are distinct, although they share some basic principles and traditions. In the next subchapters, both frameworks with respect to citizen science will be analysed.

2.5.1 Overview

2.5.1.1 General

There are already a number of policies and programmes in the EU that support and/or recognise CS. For example, the EC stated in its *Best practices in Citizen Science for Environmental Monitoring* that, among other things "EU-funded research programmes have included action to promote and support it in various thematic domains and throughout the research and innovation process".[40]

In 2002, the EC launched the 'Science and Society' Action Plan that sought to better connect science and citizens in the EU.[41] Then the 7th (2007-2013) framework programme for R&I (FP7) was born in which the EC funded a variety of projects using citizen science.[42]

2.5.1.2 Open Science

An important element of CS is that it can challenge traditional science practice by making the process more open. Not only by letting citizens participate in the production of scientific knowledge, but also by making the data and methodology publicly available.[43] In the Horizon 2020 subsidy programme for research and innovation Citizen science was strongly promoted and as a result was given a larger role in numerous cases. For instance, citizen science is closely linked to the European policy of a more open science.[44] Some other important initiatives under Horizon 2020 include: 'Science with and for Society', 'Responsible R&I, ICT programme. In Horizon Europe, the successor to Horizon 2020, citizen science will be given a more prominent role in the context of open science.[45] It is therefore "with these programmes, the Commission has confirmed the important role of citizen science in contributing to knowledge creation and trust between science and society, and to (digital) social innovation, which involves developing solutions that meet social needs through an open, participatory, bottom-up and co-creative approach."[46]

[39] Berti Suman, A., & Pierce, R. (2018). Challenges for citizen science and the EU open science agenda under the GDPR. *European Data Protection Law Review,* 4(3), 284-295. doi10.21552/edpl/2018/3/7, p. 294
[40] European Commission, COMMISSION STAF WORKING DOCUMENT, 'Best Practices in Citizen Science for Environmental Monitoring',
https://ec.europa.eu/environment/legal/reporting/pdf/best_practices_citizen_science_environmental_monitoring.pdf, p. 12
[41] See http://www.asset-scienceinsociety.eu/sites/default/files/ss_ap_en.pdf
[42] European Commission, COMMISSION STAF WORKING DOCUMENT, 'Best Practices in Citizen Science for Environmental Monitoring',
https://ec.europa.eu/environment/legal/reporting/pdf/best_practices_citizen_science_environmental_monitoring.pdf
[43] See European Citizen Science Association, 'Citizen Science & Open Science - Policy Brief is out!'. https://ecsa.citizen-science.net/blog/citizen-science-open-science-policy-brief-out
[44] Berti Suman, A., & Pierce, R. (2018). Challenges for citizen science and the EU open science agenda under the GDPR. *European Data Protection Law Review*, *4*(3), 284-295. https://doi.org/10.21552/edpl/2018/3/7
[45] European Commission, COMMISSION STAF WORKING DOCUMENT, 'Best Practices in Citizen Science for Environmental Monitoring'
https://ec.europa.eu/environment/legal/reporting/pdf/best_practices_citizen_science_environmental_monitoring.pdf, p. 12
[46] Ibid.

Other important European initiatives are: European open science agenda / European open science cloud, Open Data Strategies, Cohesion policy programmes.

Within the framework of environmental policy, CS also contributed to the implementation of the 7th environmental action programme.[47] Furthermore, there are several documents published by the EC that call for specific action on citizen science, such as 'action plan on nature, people and the economy', 'actions to streamline environmental reporting', 'action plan on environmental compliance and governance' and 'EU pollinators initiative'.[48]

2.5.1.3 Citizen science and European environmental policy

Citizen science is thus particularly well developed within the field of environmental policy. It offers a unique opportunity to expand the knowledge base by mobilising lay and local knowledge, and to promote awareness and engagement.[49] A recent study analysed in detail the added value of citizen science on environmental policy.[50]

In order to monitor the effectiveness of EU (environmental) legislation and the progress of its policy objectives, the Commission uses, among other things, the data that the Member States are obliged to collect and report to the Commission (and also the EEA in the case of environmental policy). In this way, a fitness check is carried out every so often to assess the effectiveness of this regulatory supervision for EU (environment) policy.[51] The 2017 fitness check of reporting and monitoring of EU environment policy concluded that new data sources such as those collected by the public, and therefore citizen science, could simplify and streamline reporting and monitoring. This in turn could provide a more reliable evidence base for European environmental policy.[52] There are many examples where the data of citizen science projects are being used for environmental monitoring and reporting in the context of European environmental policy (see footnote).[53]

2.5.1.4 EU fundamental rights and legislation

What follows is a discussion of the important fundamental European rights and laws in the context of citizen science and air quality.

[47] DECISION No 1386/2013/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 20 November 2013 on a General Union Environment Action Programme to 2020 'Living well, within the limits of our planet' (Text with EEA relevance). L 352/171

[48] For more information, see: European Commission, COMMISSION STAF WORKING DOCUMENT, 'Best Practices in Citizen Science for Environmental Monitoring', https://ec.europa.eu/environment/legal/reporting/pdf/best_practices_citizen_science_environmental_monitoring.pdf

[49] Haklay, M. (2013). Chapter 7 - Citizen Science and Volunteered Geographic Information: Overview and Typology of Participation. In D. Sui, S., Elwood, & M., Goodchild (Reds.). *Crowdsourcing Geographic Knowledge: Volunteered Geographic Information (VGI) in Theory and Practice* (pp. 105-122). New York: Springer.

[50] Citizen science for environmental policy: development of an EU-wide inventory and analysis of selected practices. 7 December 2018 [Online]. Available: https://publications.europa.eu/en/publication-detail/-/publication/842b73e3-fc30-11e8-a96d-01aa75ed71a1/language-en

[51] European Commission, COMMISSION STAF WORKING DOCUMENT, 'Best Practices in Citizen Science for Environmental Monitoring'
https://ec.europa.eu/environment/legal/reporting/pdf/best_practices_citizen_science_environmental_monitoring.pdf, p. 10

[52] This trend towards greater transparency and simplification of reporting within the EU was further reinforced by the entry into force of Regulation (EU) 2019/1010 on the alignment of reporting obligations in the field of legislation related to the environment.

[53] A well-known example is Birdlife, which is used to meet the reporting requirements of Article 12 of the Birds Directive and Article 17 of the Habitats Directive. See https://ec.europa.eu/environment/nature/knowledge/rep_habitats/index_en.htm en https://ec.europa.eu/environment/nature/knowledge/rep_birds/index_en.htm

2.5.1.4.1 Air quality legislation

Air pollution poses a cross-border challenge because its effects are transnational and it affects the environment and human health.[54] To combat air pollution, the European Union (EU) uses, among other things, Directives. These are legal instruments of the EU to align national legislation within countries that are members of the Union (member states). Directives relating to air quality have demonstrated that they are an essential instrument for tackling air pollution in the member states.[55]

The EU policy framework for air quality therefore consists of three pillars with different directives, namely:

- Air quality standards:
  - There are two directives for this, the aim of which is to reduce air pollution in the European Union. They do this by imposing certain requirements on the concentrations of certain substances. In order to achieve the air quality standards, these values must be continuously monitored.
    - Air Quality Directive (AAQD)[56]
    - Directive on heavy metals and polycyclic aromatic hydrocarbons in ambient air[57]
- National emission reduction targets:
  - Certain air pollutants such as sulphur dioxide, fine dust, etc. also have emission ceilings in addition to the limit values. In order to achieve this, there are two directives that set emission limits:
    - Revised National Emission reduction Commitments Directive[58]
    - Medium Combustion Plant Directive (MCPD)[59]
- Emission standards for sources of pollution:
  - This pillar regulates the sources of air pollution in the European Union. There are thus several directives that focus specifically on each sector.
    - E.g. a directive to deal with air pollution from road vehicles[60]

The AAQD is of particular interest to the SOCIO-BEE project as it deals with general air pollution in EU. It also has an impact on various people's rights and is increasingly being invoked in national and European court cases. For example, this directive (as well as others) includes a "limit value" - a limit on the level of harmful air pollution in outdoor air. The Court of Justice of the European Union is of the opinion that when

[54] European Environment Agency, 'Air Quality in Europe – 2020 Report', 9. https://www.eea.europa.eu/publications/air-quality-in-europe-2020-report

[55] European Commission, Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee, the Committee of the Regions and the European Investment Bank - A clean planet for all: A long-term European strategic vision for a prosperous, modern, competitive and climate-neutral economy [COM(2018)773 final]. Brussels, 28.11.2018.

[56] Directive 2008/50/EC of the European Parliament and of the Council of 21 May 2008 on ambient air quality and cleaner air for Europe, OJ L 152, 11.6.2008, p.1-44

[57] Directive 2004/107/EC of the European Parliament and of the Council of 15 December 2004 relating to arsenic, cadmium, mercury, nickel and polycyclic aromatic hydrocarbons in ambient air, OJ L 23, 26.1.2005, p. 3–16

[58] Directive (EU) 2016/2284 of the European Parliament and of the Council of 14 December 2016 on the reduction of national emissions of certain atmospheric pollutants, amending Directive 2003/35/EC and repealing Directive 2001/81/EC (Text with EEA relevance), OJ L 344, 17.12.2016, p. 1–31

[59] Directive (EU) 2015/2193 of the European Parliament and of the Council of 25 November 2015 on the limitation of emissions of certain pollutants into the air from medium combustion plants (Text with EEA relevance), OJ L 313, 28.11.2015, p. 1–19

[60] Directive 2009/33/EC of the European Parliament and of the Council of 23 April 2009 on the promotion of clean and energy-efficient road transport vehicles (Text with EEA relevance), OJ L 120, 15.5.2009, p. 5–12

these limit values are exceeded, legal consequences are attached to it.[61] Citizens and groups therefore have the right to demand action from governments in national courts.

Meanwhile, the European Commission is revising the AAQD as part of the Green Deal's Zero pollution action plan. It is expected that the Commission will come up with a proposal for revision of the AAQD in 2022. The other environmental legislation will also be revised in the long term, based on best practices from a recent review of the directives (fitness check).

Since this is an air quality directive, it must then be transposed and implemented in the various member states. This means that the directive can enter into force in the member states and the EC can check whether the member states are taking the right measures to achieve the targets.

Below are the various legislations that transpose and implement the AAQD into national legislation for the pilot countries of the Socio Bee project:

Greece

- Measures to improve the quality of steam Ra, in compliance with the provisions of the Directive 2008/50/EC on ambient quality air and cleaner air for Europe' of Europe the European Parliament and the Council of the European Union European Union of 21 May 2008', Εφημερίς της Κυβερνήσεως (ΦΕΚ) (Τεύχος Β) ; Number: 488 ; Publication date: 2011-03-30 ; Page: 07111-07161

Italy

- Implementation of Directive 2008/50/EC on ambient air quality and cleaner air in Europe, Gazzetta Ufficiale della Repubblica Italiana ; Number: 216 ; Publication date: 2010-09-15

Spain

It seems that Spain hasn't taken any specific measure to combat the air quality pollution in regard to the AAQD. Spain has been referred to court several times now by the EC for failing to protect citizens from poor air quality.

2.5.1.5 Towards a 'right to clean and healthy air'?

Thus, there is currently a great deal of case law at the European Union level (from the Court of Justice of the European Union) that relates to the foregoing 'limit values'. There is as yet no explicit recognition of the right to clean and healthy air in the EU legal framework, but there is a possible right to air quality "with levels of pollutants not exceeding the limit values set under Article 13 and Annex XI of the AAQD for the protection of human health".[62]

Furthermore, there are also international fundamental rights that protect individuals from the effects of air pollution. For example, air pollution can be said to deny the enjoyment of the right to private and family life, the right to health and the right to life.[63] Further work is also underway on a right to breathe clean and healthy air which serves as an essential component for the recognition of the right to a healthy and sustainable environment.[64] This report also showed, according to the UN, that all EU member states already (in)directly recognize this right through, among other things, constitutions, case law of the

[61] See Case C-59/89 Commission v Germany at §§18-19; Case C-404/13 ClientEarth, at §55-56

[62] ClientEarth, 'Individual right to clean and healthy air in the EU', p. 4, June 2021. https://www.clientearth.org/media/adtcznde/individual-right-to-clean-and-healthy-air-in-the-eu-pdf.pdf

[63] Guerra and Others v. Italy, 14967/89, [GC], (ECHR, 19 February 1998), "environmental pollution may affect individuals' well-being and prevent them from enjoying their homes in such a way as to affect their private and family life adversely"

[64] 5 Report of the Special Rapporteur on human rights and the environment to the UN General Assembly, *Right to breathe clean air*, A/HRC/40/55, 8 January 2019. https://undocs.org/A/HRC/40/55

Supreme Court/Constitutional Court or ratification of international treaties such as the Aarhus Convention.[65]

Finally, one could also interpret that jurisprudence of the European Court of Human Rights at Council of Europe level in, among others, Article 8 (Protection of the right to private and family life) and Article 2 (Protection of the right to life) has also recognized the right to a safe and healthy environment by giving health and environment a prominent place in its jurisprudence.[66]

2.5.1.6 Towards a 'right to access environmental information'?

Another potentially relevant example of fundamental rights in CS is 'Citizen Sensing'. Citizen Sensing is a subset within citizen science that is situated in the field of 'environmental monitoring and reporting' by lay citizens and it has the potential to provide CS with a legally binding dimension.[67] In citizen sensing "citizens are gathering environmental data to demonstrate environmental wrongdoings and claim their rights"[68], where it can serve as a source of evidence in environmental litigation or as a tool to mediate environmental conflicts and in the process restore trust between citizens, government and the private sector. [69] It achieves greater transparency and accountability by including citizens in risk governance and thereby "[…] essentially manifests claims based on individual rights such as the right to live in a healthy environment and the right to access environmental information".[70]

As indicated earlier, it is important that the data and technology in monitoring are of good quality if citizen science is to be seen as relevant by authorities. In practice, however, there is a lack of a legal instrument and legal foundation for this data collection from citizens that can facilitate, justify and protect the cooperation between citizens and authorities. The author Berti Suman therefore argues that citizen sensing, "as a manifestation of human rights and – in particular – of the right to access environmental information recognized by the afore-mentioned Aarhus Convention, could generate a 'duty to listen' for governmental actors, provided that certain conditions are met".[71] [72]

Research on this is still in its infancy (especially in the EU), but these developments may be relevant to the SOCIO-BEE project. For example, the data and results obtained from citizen scientist may not only change the behavior of citizens (see more environmentally conscious), but also have legal implications in terms of environmental justice and protection.

---

[65] UN Special rapporteur on human rights and the environment, *Recognition of the Right to a Healthy Environment in Constitutions, Legislation and Treaties*, (Annual thematic report, 30 December 2019), A/HRC/43/53, p. 8, at https://undocs.org/A/HRC/43/53; ClientEarth, 'Individual right to clean and healthy air in the EU', June 2021. https://www.clientearth.org/media/adtcznde/individual-right-to-clean-and-healthy-air-in-the-eu-pdf.pdf

[66] See for example dissenting opinion of Judges Costa, Ress, Turmen, Zapancic and Steiner in case Hatton and Others v. the United Kingdom [GC]

[67] Suman, A. B. (2021). Citizen Sensing from a Legal Standpoint: Legitimizing the Practice under the Aarhus Framework, *Journal for European Environmental & Planning Law*, *18*(1), 8-38. doi: https://doi.org/10.1163/18760104-18010003

[68] Schouten, C. (n.d.). Marie Curie Individual Fellowship awarded to Anna Berti Suman, researcher on 'Citizen Sensing'. Tilburg University. https://www.tilburguniversity.edu/magazine/marie-curie-individual-fellowship-awarded-anna-berti-suman

[69] Anna Berti Suman & Marina van Geenhuizen (2020) Not just noise monitoring: rethinking citizen sensing for risk-related problem-solving, *Journal of Environmental Planning and Management*, *63*(3), 546-567, doi:10.1080/09640568.2019.1598852

[70] Suman, A. B. (2021). Citizen Sensing from a Legal Standpoint: Legitimizing the Practice under the Aarhus Framework, *Journal for European Environmental & Planning Law*, *18*(1), 8-38. doi: https://doi.org/10.1163/18760104-18010003, p.9

[71] Ibid., p. 10

[72] A practical example is the Formosa litigation decided in summer 2019 by a U.S. Court. Here, citizens themselves went to work collecting citizen sensed-evidence regarding the environmental pollution caused by the factory dumping plastic into local waters and thus it violated the Clean Water Act. However, there was no official evidence of this with the relevant authorities because the company never filed a pollution declaration. See https://www.texasobserver.org/nurdle-by-nurdle-citizens-took-on-a-billion-dollar-plastic-company-and-won/. Accessed January 21, 2022.

2.5.1.6.1 Citizen science and European data policies

A core aspect of citizen science is the idea that individuals participate in data collection for further research, and some authors or projects even go so far as to allow participants to participate at all stages of the research. In any case, data plays a central role in this concept. This brings with it both potential advantages and disadvantages. Potential data challenges include data quality, different data policies and data management principles, the role of data protection and handling of sensitive information in Europe, data biases due to unbalanced demographics of participants, etc.[73] What follows are discussions on the interaction of citizen science with some of the data legislation in Europe that may affect the SOCIO-BEE project.

2.5.1.7 Citizen science, data governance and free flow of (non-)personal data in the EU

2.5.1.7.1 General Data Protection Regulation74

The General Data Protection Regulation (GDPR) was adopted in 2016 and entered into force in 2018. This instrument regulates the processing of personal data in EU as well as transfers of personal data of EU citizens and residents outside the EU. Personal data entail information relating to natural persons who can be identified or who are identifiable, directly or indirectly.

The GDPR sets out seven key principles: sets out seven key principles:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

On the account of those principles, the GDPR introduces obligations for the data controllers and processors and rights for the data subjects. Those rights include: the right to be informed, the right of access, the right to rectification, the right to erasure, the right to restrict processing, the right to data portability, the right to object and rights in relation to automated decision making and profiling.

For personal data processing to occur in a legitimate manner, the data controller and the data processor must provide for a legal basis. The legal bases are: the individual's consent, the performance of a contract, a legal obligation, vital interests, a public interest or public task and legitimate interests. the processing of special categories of data (data relating for instance to health or revealing one's sexual orientation) is in principle prohibited, unless an exemption applies.

The GDPR and the implementing national legislations will apply to the SOCIO-BEE projects, when the processing of personal data occurs. Citizen Science poses several implications with respect to the data

[73] A detailed description of possible obstacles in connection with data can be read from page 19 in https://ec.europa.eu/environment/legal/reporting/pdf/best_practices_citizen_science_environmental_monitoring.pdf

[74] 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) (Text with EEA relevance), *OJ L 119, 4.5.2016, p. 1–88.*

protection legal framework, mainly due to its openness and its decentralized character.[75] Researchers working for official research institutions or academia, in order to conduct trials and experiments, have to abide by very strict standards, for instance go through lengthy ethics procedures to have their research designs and protocols approved. Respectively, during the actual research implementation stage, research takes place usually by highly specialized experts, who have to follow precise methodologies and specific codes of conducts and principles of research integrity, retain a level of transparency, disclose information about possible conflicts of interest or funding, appropriately publish their results and ensure the datasets can be re-used to ensure repeatability and verifiability – all these in line with strict laid out legal and ethical requirements. Comparatively, in the context of citizen science, despite the existence of some underlying principles, there is a degree of informality and flexibility, leading to questions such as: who oversees a trial and who is the data controller? Can in some cases citizen science be simply a household activity which would be exempt from the GDPR application? And who can data subjects whose rights have been violated turn to?

Overall, the GDPR does provide special and sometimes seen as more privileged conditions for the processing of personal data when the latter are used in the context of scientific research, as compared to other purposes, due to a general perception that this is important for the common good.[76] Scientific research is not defined in GDPR. The European Data Protection Board has adopted Guidelines in this regard to shed light on the interplay between scientific research and data protection law, with respect to health.[77]

2.5.1.7.2 Regulation 2018/1807 on the free flow of non-personal data in the EU[78]

The main focus of this regulation is to boost the data economy by facilitating the cross-border exchange of data. The Commission published a guidance that focuses on the interplay between this new regulation and the GDPR. It addresses in particular:

- The concepts of personal and non-personal data and the concept of mixed datasets
- The principles of free movement of data and the prohibition of data localisation requirements
- Data portability.

Non-personal data can be classified as follows:

- Data which originally did not relate to an identified or identifiable natural person, e.g. data on weather conditions generated by machines
- Data which used to be personal data but were (properly) anonymised and therefore do not qualify as personal data anymore

The aforementioned Guidance makes it clearer how to deal with mixed datasets that often occur in real life such as possible with the SOCIO-BEE project e.g. “research institution's anonymised statistical data and the raw data initially collected, such as the replies of individual respondents to statistical survey

[75] A Berti Suman and R Pierce, ‘Challenges for Citizen Science and the EU Open Science Agenda under the GDPR’ (2018) 4 European Data Protection Law Review 284.
[76] Paul Quinn, ‘Research under the GDPR - a Level Playing Field for Public and Private Sector Research?’ (2021) 17 Life Sciences, Society and Policy 4.
[77] https://edpb.europa.eu/sites/default/files/files/file1/edpb_replyec_questionnaireresearch_final.pdf
[78] European Commission, ‘Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union (Text with EEA relevance.), L 303/59

questions".[79] When both types of data apply in the project, the data protection rights and obligations stemming from GDPR will fully apply to the mixed dataset.[80]

2.6 Citizen Science and Technology

Citizen science projects related to air pollution have already proven to be valuable in environmental monitoring, reporting and policy-making. Big data and new technologies are claimed to enable citizen science initiatives not only to make more efficient and reliable measurements, but also to have an impact on environmental policies and legislation, for example, by providing both new and large amounts of data that can be used as evidence for policy makers.

More and more citizen science initiatives depend on technology. Individuals use their personal devices, such as smartphones and drones, equipped with cameras and basic sensors used primarily for recreational purposes to collect information about the environment. Although several tools exist in the EU to reduce this problem, there is a growing interest in using low-cost sensors to increase the spatial resolution of monitoring at lower cost.[81]

Further, those tools become more and more advanced. In SOCIO-BEE for example, the consortium aims to equip citizen scientists with proper user-friendly tools, powered by machine learning and artificial intelligence. It is understandable that entrusting such complex technologies in the hands of non-experts, would have to be done with caution and would require prior training as well as continuous guidance and oversights.

2.7 Future developments to keep an eye on

2.7.1 Citizen science and European environmental policy and decision-making

CS practices can offer great potential in the realm of environmental policy making. Participatory processes display a long history in environmental policy-making, as acknowledged in the 1998 UN Economic Commission for Europe's 'Convention on Access to Information, Public Participation in Decision-Making and Access to Justice in Environmental Matters'[82], which establishes, inter alia, the right for everyone to receive environmental information held by public authorities and to participate in environmental decision-making. Data collection through CS initiatives can improve societal awareness and feed in the public debate on environmental issues.

In this regard, CS can contribute to the successful implementation of the European Green Deal and of other priorities set at the European level, which include public involvement and empowerment in policy-making processes[83]. Moreover, as stated by the European Commission in 2013[84], the "development of communication technologies through the internet creates highly valuable opportunities for citizen science

[79] De Smet, S., Free flow of non-personal data and GDPR, (2019, June 19). [Online]. Available : https://www.loyensloeff.com/en/en/news/news-articles/free-flow-of-non-personal-data-and-gdpr-n14929/

[80] European Commission, 'COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL EMPTY - Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union', COM(2019) 250 final, p. 9

[81] EEA Report No 19/2019 Assessing air quality through citizen science: https://www.eea.europa.eu/publications/assessing-air-quality-through-citizen-science

[82] https://unece.org/fileadmin/DAM/env/pp/documents/cep43e.pdf

[83] https://ec.europa.eu/jrc/communities/en/community/examining-use-and-practices-citizen-science-eu-policies/page/best-practices-citizen

[84] https://ec.europa.eu/environment/archives/seis/pdf/seis_implementation_en.pdf

and crowdsourcing, offering enhanced levels of participation in assessing (and determining) the success of EU environment policies".

The environmental data collected by individuals could improve coverage provided by traditional sources both in geographical and temporal terms and represent a cost-effective solution. Nevertheless, one key obstacle that CS practices have to face lies in the uptake of such data in public policy and decision-making processes. Indeed, it remains to be assessed how data spontaneously collected by citizens could be incorporated into evidence-based public authorities' decision processes. In the near future, data quality requirements by public authorities should be acknowledging the development potential offered by CS practices. SOCIO-BEE will offer much needed best practices and guidelines on how to incorporate CS data in environmental policy and decision-making, in line with Action 8 "Promote the wider use of citizen science to complement environmental reporting" of the EC 2017 "'Fitness check of reporting and monitoring of EU environment policy'[85]. Another aspect that requires further development in the upcoming years lies in the integration of CS in national and regional policies and programmes[86]. Through the creation of networks and the sharing of best practices, co-ordination and the definition of opportunities, roles and responsibilities will be guaranteed at different governance levels, hence contributing to the creation of a coherent framework across all Member States.

The SOCIO-BEE project will delve into the integration process of CS data in public policy and decision-making, with a view to increase transparency and citizen participation. In this regard, the potential of data integration will be measured against different areas of public intervention, with a focus on environmental matters, in order to maximize benefits. More specifically, the work carried out within SOCIO-BEE will focus on typical public decision-making processes, such as traffic limitations or development of green areas, and will identify which data are required to monitor the impact of specific services linked to contracts, such as local public transports. As a result, insights will be provided on data requirements in public decision-making processes and in the integration of traditional monitoring systems. The possibility to use such data in performance contracts schemes for public procurement will also be explored. In conclusion, the experience in SOCIO-BEE will contribute to gain a more thorough understanding of how participatory approaches in data collection can be transferred to public policy and decision-making processes with an impact on the environment.

Digital Services Act

Recently, the Digital Services Act was also adopted. This act will regulate digital services in the EU and tries to modernise the previous e-Commerce Directive. Specifically, it will create new legislation regarding illegal content, transparent advertising and disinformation. "Digital services include a large category of online services, from simple websites to internet infrastructure services and online platforms. The rules specified in the DSA primarily concern online intermediaries and platforms. For example, online marketplaces, social networks, content-sharing platforms, app stores, and online travel and accommodation platforms".[87] As a result, this new Act may also have implications for different Socio bee platforms, for example for the connections between different project actors. Socio Bee will use various social media channels such as Twitter and also uses apps and maintains a website with important

[85] https://ec.europa.eu/environment/legal/reporting/fc_overview_en.htm
[86] https://discovery.ucl.ac.uk/id/eprint/10058422/1/Citizen-Science.pdf
[87] European Commission, 'The Digital Services Act package', See: https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package

information. The consortium will closely monitor the developments of this act by using, among other things, the legislative train schedule of the European Parliament.[88]

Data altruism

The European Commission in the European Data Strategy supports the concept of data donation and data altruism for common good. Nevertheless, a concrete framework would need to be created to ensure that all the rights of the people who participate in such emerging initiatives. The SOCIO-BEE aims to facilitate the dialogue with the creation of guidelines and by opening up the dialogue with key policy makers and stakeholders, to accelerate relevant processes through a fundamental rights approach.[89]

2.8 Specific considerations: children and elderly persons

Since both children and elderly people participate in SOCIO BEE as citizen scientists, the consortium must take the needs of these groups into account at all times. For example, children can both learn and contribute to citizen science. "Scientific learning can develop children's environmental citizenship, voices and democratic participation as adult. The quality of data produced by children varies across projects and can be assumed to be of poorer quality because of their age, experience and less-developed skill set. If citizen science activities are appropriately designed they can be accessible to all children, which can also improve their accessibility to a wider range of citizens in general".[90]

With regard to the elderly, we see that citizen science initiatives can also help this group in their perception of autonomy, empowerment and collective agency. By taking part in citizen science-related activities, they get the feeling that they actually get to know their surroundings better and can also exert an influence on it. This in turn has the effect of making them feel significantly better. Not only the health of the elderly is improved, but also the environment in which they live can be improved if there are problems that can be addressed through citizen science. Clear and age-specific measures, together with the necessary support, ensure that this group can also participate in citizen science.[91]

2.9 Preliminary recommendations

Create a framework for Citizen Science

Citizen science has no single definition. However, to help the Socio Bee project with this, it is good to use the *The 10 Principles of Citizen Science* compiled by the European Citizen Science Association[92] as a reference point. These 10 principles are a summary of best practices that projects can meaningfully engage with. Standardisation can help when seeking funding for a project so that agencies have a better idea of what to expect from the project.

[88] European Parliament, 'Digital Services Act: adapting commercial and civil law rules for commercial entities operating online', See: https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-digital-services-act-commercial-and-civil-law-rules

[89] Call: H2020-LC-GD-2020: SOCIO-BEE, GA No: 101037648, p. 83

[90] Makuch, K.E., & Aczel, M.R. (2018). Children and citizen science. In: Hecker, S., Haklay, M., Bowser, A., Makuch, Z., Vogel, J. & Bonn, A. 2018. *Citizen Science: Innovation in Open Science, Society and Policy*. UCL Press, London. https://doi.org/10.14324/111.9781787352339

[91] King, A. C., King, D. K., Banchoff, A., Solomonov, S., Ben Natan, O., Hua, J., Gardiner, P., Rosas, L. G., Espinosa, P. R., Winter, S. J., Sheats, J., Salvo, D., Aguilar-Farias, N., Stathi, A., Akira Hino, A., Porter, M. M., & Our Voice Global Citizen Science Research Network, O. (2020). Employing Participatory Citizen Science Methods to Promote Age-Friendly Environments Worldwide. *International journal of environmental research and public health*, *17*(5), 1541. doi.org:10.3390/ijerph17051541

[92] ECSA, 'ECSA's characteristics of citizen science'. (April 2020). Available : https://ecsa.citizen-science.net/wp-content/uploads/2020/05/ecsa_characteristics_of_citizen_science_-_v1_final.pdf

Designing citizen science tools: privacy-, age, and user-friendly

As technology develops, so do the tools that citizen science projects can use. Firstly, by using user-friendly tools, complex technologies can also be used by non-experts to do qualitative scientific data collection. Concerning the research involving elderly people and aged populations, elderly persons are considered an important target group of the project, provided that its tools and equipment will be designed to be used by people of different ages and skills (for example user-friendly interfaces, easy mechanisms for data capturing and processing, simple procedures for registering in the programs offered by the platform). The SOCIO-BEE will engage elderly persons over 65 years old and whenever necessary caretakers. For children, the researchers will ensure that all equipment provided is child-proof (based on EU safety standards) and age-appropriate. With respect to the GDPR, the SOCIO BEE researchers engaging in the development of the technological aspects of the project shall observe the principles of data protection by design and by default in line with article 25 GDPR. This would include not only the actual data processing operations they will be engaged with but also the envisaged use of the platform in a real environment, as technology providers. The partners have already introduced measures which limit the possibility to collect personal data

Keep close contact with related citizen science organisations and other EU-related projects

There are many organisations worldwide, in the EU and also more and more in the Member States that are specifically concerned with citizen science. The exchange of ideas and all kinds of other questions, can lead to new answers and possibilities to future challenges, especially in the field of data and technology. Other (EU) projects related to environmental policy (or specifically air quality) are relevant to this project because of the challenges the EU faces in addressing climate change. The activist nature of citizen science, which is often linked to environment-related issues, can also be read in parallel with increasingly empowered citizens who, through national court cases in the EU, hold governments to account for their negligence. It is therefore interesting to keep an eye on how the citizen scientists deal with the data obtained from Socio Bee

Follow-up of recent developments regarding best practices

In the European Union, many studies have been published on best practices. The European institutions are also increasingly incorporating citizen science into their policies and numerous studies. Following international, European and national trends on involving citizens in science and policy can therefore provide answers to challenges that arise during a project. Also take into account the development of new technologies and their advantages and disadvantages, in general and specifically when possible for citizen science. Also academic research where citizen science is used as a methodology can bring up very useful cases. This is especially the case in the context of the GDPR and other privacy, data protection and ethical fundamental rights.

Research activities with children

In any case, all partners involved in such activities are required to provide a protocol of research at the beginning of the project, including all copies of the acquired documents, to be readily available upon request to the European Commission, as well as to the legal guardians

Especially for research involving children who are unable to make decisions for themselves, entails that researchers must maintain an active relationship with their legal guardians and/or carers. This means that the legal guardians must be allowed to monitor the activities and be in continuous communication with the researchers. Thus, all activities involving children will take place in controlled environments.

3 Use of drones in the Socio Bee context: Legal and regulatory framework

3.1 Definition of drones

A drone, or more formally known as unmanned aerial vehicle (UAV) is an aircraft without any human pilot, crew or passengers on board. Fundamentally, a drone can be remotely controlled or fly autonomously using software-controlled flight plans in its embedded systems, that work in conjunction with onboard sensors and a global positioning system. Initially drones were mostly associated with military applications, however nowadays drones are used in a range of civilian roles, including search and rescue, surveillance, traffic monitoring, weather monitoring, firefighting, personal recreational use, drone-based photography and videography and agriculture. The rapid adoption of drones over the past decade has sparked privacy, security and safety concerns. Maliciously drones can be used to obtain images of people in their homes and other locations once assumed to be private. Furthermore, the increased use of commercial and personal drones has also raised the potential for midair collisions and loss of drone control. Specific concerns about drones flying over people or too close to commercial aircrafts have prompted calls for regulation.

3.2 Definition of drones in Socio Bee

In the context of air quality monitoring certain areas (industrial, rural) may turn out as a very challenging task for citizens, as their mobility can be hindered by obstacles. The most efficient way to collect data is to implement mobile pollution monitoring by using drones. In SOCIOBEE approach, one of the innovations is to utilize wearable modular air pollution sensors as modules that can be attached to devices such as recreational drones. This offers the opportunity to scan relatively large areas with the capability to create 3D pollution maps, that is either not possible or too expensive with neither wearables or stationary pollution monitoring networks.

3.3 The international framework

3.3.1 United Nations

At international level, there is the International Civil Aviation Organisation (ICAO). This is a specialised agency of the UN that serves as a diplomatic platform where air transport policy and the principles, techniques, standards etc. for international air navigation are discussed and established (albeit not binding on national governments).[93] It was established by the 1944 Convention on International Civil Aviation (also known as the 'Chicago Convention')[94]. This convention has served to date to create more uniformity worldwide in terms of regulation and cooperation, etc.[95] An important provision here is the Remotely Piloted Aircraft Systems introduced in 2011.[96] Since a new Circular 328, UAVs are also covered by the Chicago Convention, albeit only in the context of the Remotely Piloted Aircraft Systems (RPAS).[97] This means that a 'drone' is part of the RPAS and therefore always controlled from a distance and never autonomously. All European Member States are also members of ICAO and therefore try to follow ICAO rules as closely as possible, even though they are not binding. An important aspect of the UAV section in

[93] See: https://www.icao.int/about-icao/Pages/default.aspx
[94] See: https://www.icao.int/about-icao/History/Pages/default.aspx
[95] Art. 37 of the Chicago Convention
[96] ICAO (2011), Unmanned Aircraft Systems (UAS), Cir.328.AN/190, Montreal.
[97] Ibid., p. 3

the Convention is that it does not apply to UAVs intended for recreational use.[98] Furthermore, in 2015 ICAO has published a Manual (ICAO, 2015) "which is to constitute the basis for regulations regarding RPAS in the international airspace. Chapter 3 of the Manual stresses that the operation of an RPA within the boundaries of its State of Registry remains under the purview of the respective national authority".[99]

3.4 The EU framework

3.4.1 Key organisation in EU

"European Union Aviation Safety Agency (EASA) is an Agency of the European Union. As an EU Agency, EASA is a body governed by European public law; it is distinct from the Community Institutions (Council, Parliament, Commission, etc.) and has its own legal personality. The Agency develops common safety and environmental rules at the European level. It monitors the implementation of standards through inspections in the Member States and provides the necessary technical expertise, training and research. The Agency works hand in hand with the national authorities which continue to carry out many operational tasks, such as certification of individual aircraft or licensing of pilots". [100] It is the "centrepiece of the European Union's strategy for aviation safety".[101]

With the initial EASA Basic Regulation[102], EASA was established and was given responsibilities that would expand over the years.

3.4.2 Previously applicable legislation

3.4.2.1 Regulation 216/2008 on Common Rules in the Field of Civil Aviation

Regulation 216/2008 on Common Rules in the Field of Civil Aviation included Unmanned Aerial Vehicle (UAV) and defined as follows: "Unmanned aircraft . . . which includes any aircraft operated or designed to be operated without a pilot on board". "The Regulation granted the EASA the competence to regulate all aircraft with a maximum take-off mass of more than 150 kg along with the authority for Implementing Rules dealing with airworthiness certification, continuing airworthiness, operations, pilot licensing, air traffic management and aerodromes." [103] These meant that UAV's with a mass of less than 150 kg were under the competence of EU member states.

3.4.2.2 Riga Declaration and Notice of Proposed Amendment

The regulatory framework in Europe had been fragmented by diverging legislative bodies that might have impeded the emergence of a harmonised and robust civil market for UVAs. The Riga Declaration on Remotely Piloted Aircraft recognised this problem and thereby developed guidelines for the future regulation of UVAs.[104] Following this, EASA published two Advanced Notice of Proposed Amendments (A-

[98] Ibid., p. 3
[99] Mateusz, G. (2018). Analysis of international law on Unmanned Aerial Vehicles through the prism of European Union law, *Przegląd Europejski*, *2018*(4). Doi:10.5604/01.3001.0013.3455, p. 76; See also: ICAO (2015), Manual on Remotely Piloted Aircraft Systems (RPAS), First Edition, Quebec., p. 41
[100] https://www.easa.europa.eu/the-agency/faqs/agency#category-about-easa
[101] ALADDIN [Project 740859], D3.1 – Data protection, Social, Ethical and Legal Frameworks, p. 31; Regulation (EC) 216/2008
[102] Regulation (EC) No 1592/2002 of 15 July 2002
[103] This didn't apply to State Aircrafts (e.g. military, firefighting, …); ibid., p. 32
[104] This statement, adopted on 6 March 2015 by representatives of the Commission, civil aviation officials, national data protection authorities and industry representatives. Ibid., p. 32

NPA) to introduce the regulatory framework for drone operations. EASA introduced the groundwork for the future regulations for UVA's in Europe.[105]

3.4.2.3 Regulation (EU) 1139/2018 (EASA basic regulation)

It consolidated the scope of European Union competence to cover the full spectrum of the aviation landscape and reinforce the European aviation system as a whole. [106] This basic regulation extends the European competence to all civil UAS (so for example also helicopters, multicopters, etc., as long as it is unmanned).[107]

3.4.3 Current and applicable framework

3.4.3.1 Regulations (EU) 2019/947108 and 2019/945109

From 31 December 2020, the new European regulatory framework for drones will apply to all existing and future drone activities. This framework, based on *Regulations (EU) 2019/947 and 2019/945,* will ensure the safe operation of civilian drones in European airspace[110], as well as facilitate the development of innovative applications and the creation of a European market for unmanned aerial services. It will also facilitate the enforcement of citizens' privacy rights and help address security and environmental concerns for the benefit of EU citizens. Finally, it will allow the introduction of an unmanned traffic management system, U-Space, to support the development of drone operations in low-level airspace, beyond the line of sight and in congested areas such as urban areas / cities. An essential element in this framework is that they do not distinguish between recreational or commercial civil drone activities by adopting a risk-based approach.

Two important principles apply to this framework for the SOCIO-BEE:

- Adopting a risk-based and proportionate approach for drones

The new framework will introduce three categories of operations (open, specific and certified) according to the level of risks involved. A different regulatory approach will be adopted for each category.

- Flexibility regime for the Member States

[105] There also was a prototype Commission Regulation on Unmanned Aircraft Operations that was published for two categories in 2016 ('open' and 'specific').
[106] Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91.
[107] The only exception are certain small tethered aircraft in Annex I of the Basic Regulation which will remain under national competence. The Basic Regulation continues not to apply to aircraft while carrying out military, customs, police, search and rescue, firefighting, border control, coastguard or similar activities or services, nor to several aircraft mentioned in Annex I to the Basic Regulation. However, a novelty of the new Basic Regulation is the introduction of the possibility for changes in scope due to the operation of several opt-in and opt-out possibilities.
[108] Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on the rules and procedures for the operation of unmanned aircraft, OJ L 152, 11.6.2019, p. 45–71
[109] Commission Delegated Regulation (EU) 2019/945 of 12 March 2019 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems, OJ L 152, 11.6.2019, p. 1–40
[110] "One of the primary objectives of the legislation is to address certain safety issues that the widespread use of UAVs increasing create. These can be divided into two categories: 1) Air risk (collision with other aircraft, manned or unmanned); 2) ground risk (collision with persons or critical infrastructure)." ALADDIN [Project 740859], D3.1 – Data protection, Social, Ethical and Legal Frameworks, p. 34

It is not possible for member states to maintain their national drone regulation in parallel with the new European drone regulation since 31 December 2020. However, the European Regulation does provide some flexibility for the member states to develop acts to define certain aspects such as:

- Minimum age for remote pilot
- Conversion of certificates issued before the applicability of the EU regulation
- Authorisation of model club and associations
- Fines when breaching the regulation
- Use of geographical zones (UAS zone)
- Insurance
- Registration and authorization
- "To lay down national rules to make subject to certain conditions the operations of unmanned aircraft for reasons falling outside the scope of Regulation (EU) 2018/1139, including public security or protection of privacy and personal data in accordance with the Union law".[111]

The regulatory framework for drones is still in ongoing legislative process. For a brief overview of the most recent EU legislation on drones see Eurocontrol's training zone [resource in footnote].[112] To better understand this ongoing process and what the implications are of the two main EU legislation for the project, a clear distinction is made between the two preceding regulations below.[113]

3.4.3.2 Implementing Act 2020/639 114

This refers to Regulation (EU) 2019/947, which is amended by Commission Implementing Regulation (EU) 2020/639, Commission Implementing Regulation (EU) 2020/746, and Commission Implementing Regulation (EU) 2021/1166. The latest amendment involved a postponement of the date of application for standard scenarios.

This regulation is related to the operation and registration of drones. Therefore, three things are taken into account: the weight, the specifications of the civilian drone and the operation it is intended to conduct.

3.4.3.2.1 Three categories

As for the three categories, a brief description as follows according to EASA[115]:

- 'Open Category'[116]

"The 'open' category addresses the lower-risk civil drone operations in , where safety is ensured provided the civil drone operator complies with the relevant requirements for its intended operation. This category is subdivided into three subcategories, namely A1, A2 and A3. Operational risks in the 'open' category are considered low and, therefore, no operational authorisation is required before starting a flight".

[111] Cover Regulation to implementing Regulation (EU) 2019/947., p. 17
[112] https://trainingzone.eurocontrol.int/clix/securedata/FB66SMB5niEgZ1eWvNY2L5yibh6-xcyQho_o2DyqnAzN5FTCBZheMfKjDkYm6qBeqGGYKWcqsgX383Y4jT9NGaC21PdHzs0VZmVsYmrgPrw.pdf
[113] For a clear overview of both the general provisions and the latest changes, see EASA's Easy Access Rules for Unmanned Aircraft Systems. https://www.easa.europa.eu/document-library/easy-access-rules/easy-access-rules-unmanned-aircraft-systems-regulation-eu
[114] Commission implementing rules can be divided in two different types of acts. This is due to the Lisbon Treaty. The different adoption procedures of the DA and IA at the level of the EC do not affect the EASA rulemaking procedures.
[115] EASA, Civil drones (unmanned aircraft), https://www.easa.europa.eu/domains/civil-drones
[116] Ibid., Art. 4 Regulation (EU) 2019/947; article 20 of EU Regulation 2019/947; Annex part A and Article 5(1) of EU Regulation 2019/947, Part 1 to 5 Annex of EU regulation 2019/945

- 'Specific'[117]

"The 'specific' category covers riskier civil drone operations, where safety is ensured by the drone operator by obtaining an operational authorisation from the national competent authority before starting the operation. To obtain the operational authorisation, the drone operator is required to conduct a risk assessment, which will determine the requirements necessary for the safe operation of the civil drone(s)".

- 'Certified'[118]

"In the 'certified' category, the safety risk is considerably high; therefore, the certification of the drone operator and its drone, as well as the licensing of the remote pilot(s), is always required to ensure safety".

Since recreational drones will be used in SOCIO-BEE and can be made available to citizen scientists in an accessible way, they will likely fall under the 'Open Category' and in special cases under 'Specific category'. This category is therefore the main reference for most recreational drone activities and low-risk commercial activities.

3.4.3.2.2 Licensing and flight requirements

Drone operator and remote pilot

It is first important to further explain the distinction between some things for the next part. A conceptual distinction is made between a *drone operator* and a *remote pilot*. The former is the person that is registered and is also responsible for the operation at all times. This person is the owner of the drone. The latter is the person that controls the drone. They can be two different persons, but most of the time the drone operator is also the remote pilot. It is also possible that the drone operator employs one or more remote pilots (when the operator is an organization or enterprise). The remote pilot must have undergone the appropriate training for the operation to be conducted.

Registration

With the new drone regulation, there are two types of registration in the EU.

- Registration of the UAV operator
- Registration of the drone

Only drones that belong to the Certified Category need to be registered in the EU which means only the registration of the operator is relevant to the SOCIO-BEE project.

From the below table, at least one condition must be met to register the drone as stated in the Delegated Act, namely:

- The drone that is used weighs at least 250 grams or more OR achieves a kinetic energy of more than 80 joules if it were to strike a human being
- The drone that is used is equipped with a sensor / camera AND is not a toy drone as described in Directive 2009/48/EC[119]; (see further chapter privacy and data protection law)
    - A toy drone with a sensor or camera is therefor not required to be registered

[117] Ibid., Art. 5 Regulation (EU) 2019/947
[118] Ibid., Art. 6 Regulation (EU) 2019/947
[119] Directive 2009/48/EC of the European Parliament and of the Council of 18 June 2009 on the safety of toys (OJ L 170, 30.6.2009, p. 1)

Each Member State has its own online platform where operators can register.[120] Drone flights for open category do not, in principle, need to be reported to national authorities unless they are flying in UAS zones.

Training and registration

The training you need to do depends on your type of drone. The transition period lasts until 31 December 2022, which allows Member States to determine the appropriate training requirements for remote pilots according to the following table:

UAS		Operation		Drone Operator/pilot		
Class	MTOM	Subcategory	Operational restrictions	Drone Operator registration	Remote pilot competence	Remote pilot minimum age
Privately built	< 250 g	A1	- may fly over uninvolved people (should be avoided when possible)	No, unless camera / sensor on board **and** a drone is not a toy	- no training needed	No minimum age
0		(can also fly in subcategory A3)	- no flying over assemblies of people		- read user's manual	16*
						no minimum age if drone is a toy
Legacy drones (Art. 20)						16*
1	< 900 g		- No flying expected over uninvolved people (if it happens, should be minimised)	Yes	- read user's manual	16*
			- no flying over assemblies of people		- complete online training	
					- pass online theoretical exam	
2	< 4 kg	A2	- no flying over uninvolved people	Yes	- read user's manual	16*
			- keep horizontal distance of 30 m from uninvolved people		- complete online training	
		(can also fly in subcategory A3)	(this can be reduced to 5 m if low speed function is activated)		- pass online theoretical exam	
					- conduct and declare a self-practical training	
					- pass a written exam at the NAA (or at recognized entity)	
3	< 25 kg	A3	- do not fly near people	Yes	- read user's manual	16*
4			- fly outside of urban areas (150 m distance)		- complete online training	
Privately built					- pass online theoretical exam	
Legacy drones (art. 20)						

Table 1. The appropriate training requirements for remote pilots

As of 1 January 2023, remote pilot training must be conducted in accordance with EASA rules. However, most Member States already provide training that is in line with EU regulation (See table 2 '_Summary of Drone Flight Operation Requirements for 'open' category').

[120] For natural persons, typical data required in each Member State include: full name; data of birth; address; mail address and phone number; number of the insurance policy; …

Insurance

A drone operator is always required to have an insurance for the drone if they are using a drone with a weight above 20kg. However most of EASA Member States mandate a third party insurance also if you are operating a lighter drone.[121] The insurance has to be requested at the time of the application for registration.

3.4.3.2.3 Safety requirements from Implementing Act 2020/639

Flying above people

Depending on the category of the drone, there are different rules for flying over people. These will be clearly set out in a table later on. It is important to know first what the differences are between non-involved persons and a gathering of persons, as these play a role in the regulations to fly over people or not. In any case, no flights should ever be carried out in the vicinity of, or in, an emergency area.

What is an uninvolved person?[122]

An uninvolved person is a person who does not participate in the UAS operation or who is not aware of the UAS operator's instructions and safety rules.

Examples of non-involved persons:

1. Spectators gathered for sporting events, concerts or other mass events;
2. Persons present on a beach, in a park or in the street.

An uninvolved person is not only a person directly exposed to a UAS, but may also be a person in a bus, car, etc. who is indirectly exposed. For example, if a UAS flies over a car, its driver should be considered an "uninvolved person" because the UAS flying near a car may distract its driver and cause an accident.

What is a gathering of people?[123]

A gathering of people is not defined by a specific number of people, but is related to the possibility of an individual to move in order to avoid being hit by the UAS in an accident. If a group of people is so close together that the possibility to flee or walk away from the UAS is limited, this group is considered as a gathering of people. It is the responsibility of the pilot to determine whether the persons are so close together that they cannot move to safety if the UAS is lost.

Can be considered as meetings of people:

3. Sports, cultural, religious or political events
4. Beaches or parks on a sunny day
5. The shopping streets during the opening hours of the shops.

Visual Line of Sight (VLOS)

Visual Line of Sight (VLOS) “operations are a type of UAS operation in which the remote pilot maintains continuous, unaided visual contact with the unmanned aircraft. In its simplest term, the aircraft must

[121] EASA, 'Drones (UAS) FAQ’, [Online]. Available: https://www.easa.europa.eu/the-agency/faqs/drones-uas; Regulation (EU) 2019/947, Article 14 (2) (d)
[122] EASA, 'Drones (UAS) FAQ’, [Online]. Available: https://www.easa.europa.eu/the-agency/faqs/drones-uas; Regulation (EU) 2019/947, *GM1 Article 2(18) Definitions, ED Decision 2019/021/R*
[123] Ibid.

always be visible to the pilot".[124] On the other hand, you also have the Beyond Visual Line of Sight (BVLOS) where the drone is flown without the pilot having a visual line of sight to the aircraft at all times. Instead, the pilot controls the UAV using instruments from the Remote Pilot Station (RPS) / Ground Control Station (GCS). Depending on the type of drone within the 'open category', there are different rules regarding the VLOS.

At VLOS, the following are mandatory during a drone operation:

- The drone must be clearly visible at all times, including at night[125]. Night flights are allowed in the Open category if these operations fulfil all the conditions of this category.
- The drone must be equipped with a light to ensure its visibility in the air at all times. From 1 July 2022, a green flashing light will be mandatory.
- The flight environment must ensure that visibility is maintained throughout the operation

Maximum height

The regulation sets a maximum height of 120 m from the Earth's surface.[126] The illustration below from the regulation shows the situation with obstacles and hilly areas.

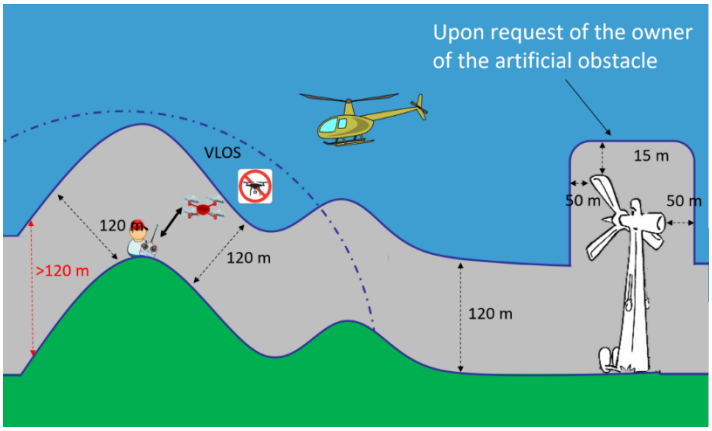

Figure 1. Maximum height of drones 'open' category[127]

The above illustration shows that if there are obstacles higher than 120 metres, you may fly up to 15 metres above them. It is important that it's only possible if there is an explicit request from the owner of the obstacle (e.g. a contract with the owner to perform an inspection). In such a case, you may fly within a horizontal distance of 50 metres from the obstacle.[128]

When you are operating in hilly environments, the height of the drone above the surface of the earth should be within the grey zone in the picture above: you need to keep the drone within 120 m of the closest point of the terrain. This means that there may be conditions such as on top of a hill where even

[124] The Soarizon Team, *'What are VLOS, EVLOS and BVLOS? Why do they affect drone operation?*, September 10, 2020. [Online]. Available: https://www.soarizon.io/news/what-are-vlos-evlos-and-bvlos-why-do-they-affect-drone-operations
[125] Night means the hours between the end of evening civil twilight and the beginning of morning civil twilight.
[126] It is possible that other values apply in Geo-Zones. See next section on Delegated Act.
[127] Source: UAS.OPEN.010 (2) (3) Annex Part A of EU Regulation 2019/947
[128] EASA, 'Drones (UAS) FAQ', [Online]. Available: https://www.easa.europa.eu/the-agency/faqs/drones-uas; Regulation (EU) 2019/947, UAS.OPEN.010 (2) (3) Annex Part A

if you keep your drone 120 m from the side of the hill, you are actually flying at a distance higher than 120 m above the bottom of the valley.[129]

Flight in urban areas for open categories

With the expected increasing crowding of drones in urban areas combined with a lot of potential risks, EASA published in April 2020 a first set of rules related to safe drone operations in European cities. In doing so, EASA sought to "balance the desire to maximise the commercial benefits and ease of use of drones with the need to ensure the safety and privacy of citizens and the potential environmental impact in our cities".130 This opinion of EASA proposed a new regulatory framework that would be the basis for the later U-space regulatory framework dealing with the management of unmanned aircraft traffic (to be discussed later in this deliverable).

Drones in the open category are allowed to fly in cities, but they must be careful of their surroundings. This certainly applies to persons in the vicinity of the place of flight. The drone operator must observe the minimum distance from persons or buildings prescribed by the regulations. Additional conditions may also be imposed in the context of geographical UAS zones.

3.4.3.3 Delegated Act 2020/1058)

This refers to Regulation (EU) 2019/945, which is amended by *Commission Delegated Regulation (EU) 2020/1058*. The latest amendment involved the introduction of two new unmanned aircraft systems classes. This regulation is related to the Requirements related to CE marking (minimal) technical requirements, maintenance of UAS and third-country operators.

3.4.3.3.1 Important minimum conditions and safety requirements from the DA

The DA describes several minimum conditions that a drone must meet. Some of the important issues for the 'open category' include:

- Does it have a Cx mark?
- Does it have an Electronic ID (real-time broadcast)?
- Does it convey a Geo-awareness?

Cx-label

The Cx-label is a new class identification table that will become mandatory for drones. It is a market product legislation to ensure compliance with certain technical requirements for unmanned aerial vehicles in the open category as laid down in Regulation (EU) 2019/945. It will be easily recognisable because the logo corresponding to the class to which it belongs is printed on the UAS and on its packaging. For example, for class C0:

[129] Ibid.

[130] EASA, 'EASA publishes first rules for safe drone operations in Europe's cities', April, 6 (2020). [Online]. Available: https://www.easa.europa.eu/newsroom-and-events/press-releases/easa-publishes-first-rules-safe-drone-operations-europes-cities

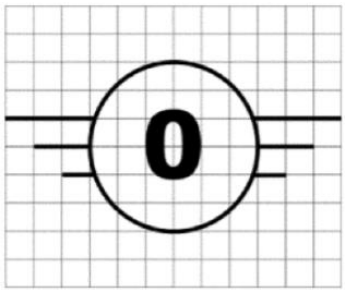

Figure 2. C0 label

There will be a total of 7 classes, from C0 to c6. More information at the end of the chapter with an overview table. Private drones are drones made by a person [that are composed of sets of components that are marketed as a ready-made kit and that are intended solely for personal use. This is not covered by the Cx label.

3.4.3.3.2 Electronic ID

The drone contains a transmitter that will continuously send out a signal with the following data:

- Operator registration number
- Aircraft serial number
- Position and height of the aircraft in relation to the ground (AGL)
- Direction and speed over ground
- Position of the pilot or position of take-off

3.4.3.3.3 Geo-awareness

This function allows knowing the exact location of the aircraft at all times. The pilot will then be able to derive the following information at all times:

- The pilot must be able to receive warnings and consult a map with the no-fly zones at all times
- Geo-fencing is not mandatory (blocking the drone where it is not allowed/can not fly)
- Pilot is responsible for the accuracy of the data for each flight (make map updates available on the drone)

3.4.3.3.4 UAS zones

As described in the Regulation, the notion 'UAS zone' means "a portion of airspace established by the competent authority that facilitates, restricts or excludes UAS operations in order to address risks pertaining to safety, privacy, protection of personal data, security or the environment, arising from UAS operations".[131][132] The flexibility regime states that EASA member states determine these UAS zones.[133] Flight authorization is needed in case the drone operation will be made in a restricted zone. Flight operation is not the same as operational authorisation. The former is for all UAVs in the open and specific category and is issued by the competent entity that is affected in the UAS zones. Operation authorisation, on the other hand, is only valid for the specific category in certain cases.

[131] Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on the rules and procedures for the operation of unmanned aircraft, OJ L 152, 11.6.2019, Art 2, (4), p. 19
[132] In addition, you are not allowed to fly a drone close to or inside an area where there is an ongoing emergency response.
[133] Article 15 and UAS.OPEN.060 (4) of EU regulation 2019/947

3.4.3.3.5 Important note: the transition period

The transition period lasts until 31 December 2022. From 1 June 2023, only drones that comply with the class identification table (i.e. C0, C1, C2, C3, C4) may be flown. These will be available on the market from 2022. However, two exceptions are possible. If the drone is purchased before 1 January 2023, the following drones can still be flown:

- A UAS of less than 250 g shall follow the rules for Category A1
- A UAS of 250 g to 25 kg follows the rules for category A3

For a UAS without a class label of less than 2 kg (but more than 250 g) it will no longer be allowed to fly at a distance of less than 50 m from people (as for category A2).

Table 2. Summary of Drone Flight Operation Requirements for 'open' category[134]

OPEN CATEGORY: not over assemblies of people; up to 120m above the ground* **VLOS/EVLOS only, except in follow-me mode within 50m distance from pilot; not drop any material**							
Operation		**Remote pilot competency**	**UAS**				**UAS operator registration**
Sub-Cat.	**Area of operation**		**Class**	**MTOM / Joule**	**Main technical requirements (CE marking)**	**Remote ID & geo-awareness**	
A1 Fly over people	You can fly over uninvolved people (not over assemblies)	• Minimum age to be set by Member States between 12 and 16 • No minimum age for privately build drone or true toy drone marked as C0 • Familiarised with the user's manual	Non-Cx compliant**	< 250g	N/A	No	No, not for true toy drones or for as long as not equipped with a camera 250g or 80J impact
			Privately build		Max speed 19m/s		
			C0 ('toy drone')		Max speed 19m/s, max attainable height above the take-off point of 120m, no sharp edges, follow-me within max 50m		
	You cannot intentionally fly over uninvolved people	• Minimum age to be set by Member States between 12 and 16 • Familiarised with the user's manual • On-line theoretical knowledge examination (with *Proof of completion of on-line theoretical knowledge examination*)	**C1** ('hobby drone')	< 80J impact at V_{term} or <900g	Max speed 19m/s, max height above the take-off point of 120m or selectable and visualised height limitation, no sharp edges, follow-me within max 50m, mechanical strength, lost-link management, geo-awareness pilot warning, battery warning, be equipped with green lights, max sound power level	Yes + unique SN for identification	Yes

A2 Fly close to people	You cannot fly over uninvolved people and need to keep a safe horizontal distance of 30m from them, reduced to 5m when flying in low speed mode	• Minimum age to be set by Member States between 12 and 16
		• Familiarised with the user's manual
		• Hold a certificate of remote pilot competency after:
		  • Online examination (idem as for cat A1/C1)
		  • Declaring practical self-training
		  • Additional cat A2 theoretical knowledge examination (in classroom, with *Certificate of remote pilot competency*)
			C2 ('prosumer drone')	< 4kg	Max height above the take-off point of 120m or selectable and visualised height limitation, no sharp edges, mechanical strength, lost-link management, geo-awareness pilot warning, low-speed mode (3m/s), battery warning, max sound power level, be equipped with green lights, protected C2 link		

A3 Fly far from people	You should: • fly in an area where it is reasonably expected that no uninvolved people will be endangered • keep a safe horizontal distance of 150m from residential, commercial, industrial or recreational areas	• Minimum age to be set by Member States between 12 and 16 • Familiarised with the user's manual • On-line theoretical knowledge examination (with *Proof of completion of on-line theoretical knowledge examination*) (idem as for cat A1/C1)	**C2** ('prosumer drone')	< 4kg	Max height above the take-off point of 120m or selectable and visualised height limitation, no sharp edges, mechanical strength, lost-link management, geo-awareness pilot warning, low-speed mode (3m/s), battery warning, max sound power level, be equipped with green lights, protected C2 link		
			C3 ('professional')	< 25kg < 3m in size	Max height above the take-off point of 120m or selectable and visualised height limitation, mechanical strength, lost-link management, geo-awareness pilot warning, battery warning, max sound power level, be equipped with green lights, protected C2 link		
			C4 (aero-model)	< 25kg	No automatic flight, lost-link management	if required by zone of operations	
			Privately build or non-Cx compliant**		N/A		

*: Exception: when flying a drone within a horizontal distance of 50m from an artificial obstacle taller than 105m, the maximum height of the operation may be increased up to 15 meters above the height of the obstacle at the request of the entity responsible for the obstacle
**: Only valid when the non-Cx drone has been put on the market by its manufacturer before January 1st 2023
JDM220620

[134] Source: "New EU drone rules What will change for everyone?", De Muyt, J.-P., 2020, June 24. Consulted from https://euka.flandersmake.be/wp-content/uploads/2020/06/local-copy-EUKA-Session-June-24th.pd

3.4.3.4 U-Space regulatory framework

The "U-Space" framework is an initiative of the Single European Sky Air traffic management Research Joint Undertaking, funded by the European Commission.[135] The U-space framework "comprises an extensive and scalable range of services relying on agreed EU standards and delivered by service providers"[136] and is designed to "support safe, efficient and secure access to airspace for large numbers of UAS (e.g. registration, electronic identification, geofencing, flight approval, tracking, etc.)".[137] The framework works in conjunction with the new *Implementing Regulation 2021/664 on the U-Space Regulatory Framework* to provide a comprehensive spatial and regulatory environment in which very-low level operations can take place.[138] [139]

In the long term every operator will have to become customer of a U-space Service Provider of choice, in an open competitive market. The gradual introduction of U-space is related to the increasing availability of blocks of services and supporting technologies. In this way, four different phases are planned[140]:

1. **U-space foundation services** provide e-registration, e-identification and geofencing
2. **U-space initial services** support the management of drone operations and may include flight planning, flight approval, tracking, airspace dynamic information, and procedural interfaces with air traffic control
3. **U-space advanced services** support more complex operations in dense areas and may include capacity management and assistance for conflict detection. Indeed, the availability of automated 'detect and avoid' functionalities, in addition to more reliable means of communication, will lead to a significant increase of operations in all environments
4. **U-space full services**, particularly services offering integrated interfaces with manned aviation, support the full operational capability of U-space and will rely on very high level of automation, connectivity and digitalisation for both the drone and the U-space system

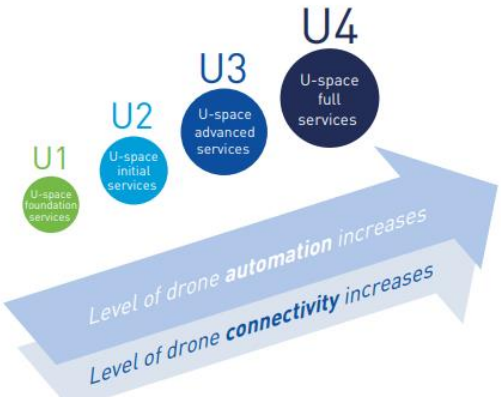

Figure 3. U-Space roll out scheme[141]

[135] See "U-Space Blueprint" (June 9, 2017), https://www.sesarju.eu/u-space-blueprint.91
[136] Ibid.
[137] NPA-A, pg. 12
[138] VLL refers to the portion of airspace below the minimum height allowed for visual flight rules (VFR) flights (typically 500 ft).) airspace operations can take place.
[139] ALADDIN [Project 740859], D3.1 – Data protection, Social, Ethical and Legal Frameworks, p. 36
[140] SESARJU, "U-Space Blueprint" (June 9, 2017), p. 5
[141] See "U-Space Blueprint" (June 9, 2017), https://www.sesarju.eu/u-space-blueprint.91

In April 2021, the Commission published the new *Implementing Regulation 2021/664 on the U-Space Regulatory Framework*[142] that will enable the start of the U2 phase.

Finally, the image below provides an overview of the different fields of view that are important for drones. The most important frame is that of 'open' with 'VLOS' for SOCIO-BEE.

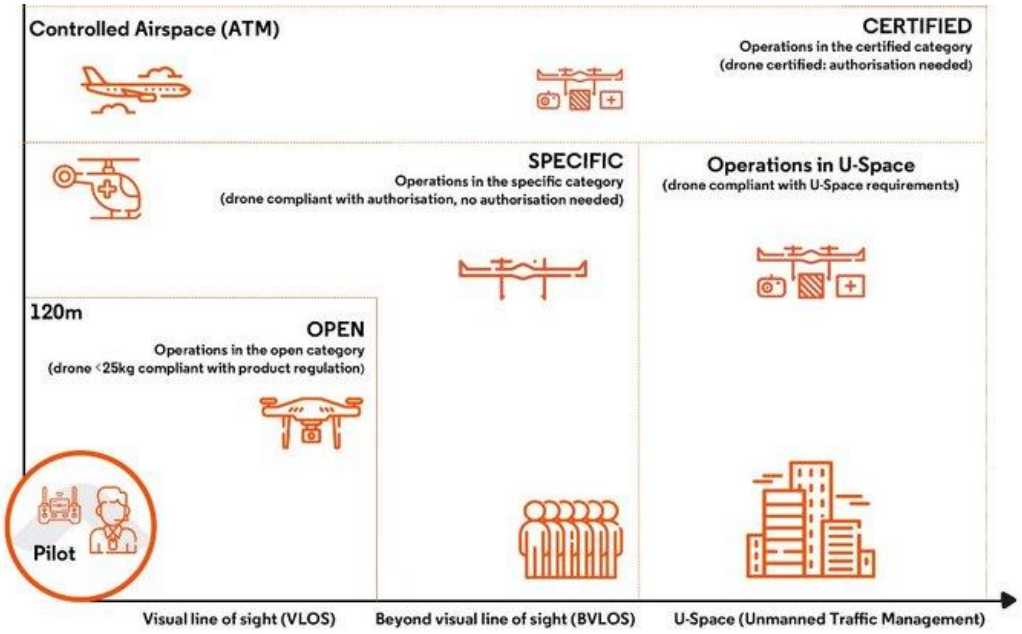

Figure 4. Overview different types of airspace for UAV

3.4.3.5 Privacy and data protection law

Due to the versatility of drones, there are many possible implications related to fundamental rights, including the right to privacy and data protection. [143] [144] For example, Cavoukian and Eleonora argue that the use of drones may "affect the right to dignity, pursuant to Art. 1 of the EU Charter of fundamental rights, much as freedom of assembly and association (Art. 12), non-discrimination (Art. 21), down to accountability and voyeurism, transparency, surveillance, and other possible infringements of data protection right by GDPR including profiling and geo-localization".[145] [146]

3.4.3.5.1 Regulation (EU) 2018/1139

The Basic Regulation clearly defines the threats to privacy and data protection in terms of the GDPR: "The rules regarding unmanned aircraft should contribute to achieving compliance with relevant rights

[142] Commission Implementing Regulation (EU) 2021/664 of 22 April 2021 on a regulatory framework for the U-space (Text with EEA relevance), C/2021/2671; OJ L 139, 23.4.2021, p. 161-183
[143] Finn, R.L., Wright, D. (2016). Privacy, data protection and ethics for civil drone practice: a survey of industry, regulators and civil society organisations. *Comp. Law & Sec. Rev.* 32, 577–586
[144] Finn, R.L., Donovan, A. (2016). *Big data, drone data: privacy and ethical impacts of the intersection between big data and civil drone deployments.* In: Custers, B. (ed.) The Future of Drone Use. Opportunities and Threats from Ethical and Legal Perspectives, pp. 47–70. Asser Press: The Hague
[145] Cavoukian, A. (2012). Privacy and Drones: Unmanned Aerial Vehicles. Information and Privacy Commissioner, Ontario
[146] Eleonora, B. (2020). From here to 2023: Civil drones operations and the setting of new legal rules for the european single sky. *Journal of Intelligent & Robotic Systems,* 100(2), 493-503. doi:10.1007/s10846-020-01185-1, p. 499

guaranteed under Union Law, and in particular the right to respect for private and family life, set out in Article 7 of the Charter of Fundamental Rights of the European Union, and with the right to protection of personal data, set out in Article 8 of that Charter and in Article 16 Treaty on the Functioning of the European Union (TFEU), and regulated by Regulation (EU) 2016/679 of the European Parliament and of the Council".[147]

It also clearly states that measures must be taken regarding *privacy by design*[148] and *privacy by default*[149] in accordance with Article 25 of the GDPR. [150]

With regard to privacy by design and default, Article 29 Data Protection Working Party "Opinion 01/2015 on privacy and data protection issues relating to the utilisation of drones" developed three principles for drone developers and operators. These three are: "(1) endorse both the principle of privacy by design and by default; (2) involve data protection officers in the design and implementation of such principles; and, (3) promote the adoption of Codes on conduct"[151] and also recommends privacy seals and marks that serve as "as a means towards accountability and compliance".[152]

3.4.3.5.2 Regulation (EU) 2019/945 & Regulation (EU) 2019/947

"UAS rules should contribute as much as possible to respecting the right to privacy and family life".[153]

The two new regulations (Regulation (EU) 2019/945 & Regulation (EU) 2019/947) intend to not only address safety risks but also security and privacy risks. The aforementioned issues such as registration, electronic identification, geofencing, UAS zones, basic knowledge from the pilot regarding safety requirements and privacy and data protection, etc. provide the basis to address for security and privacy risks.

The technical necessities introduced can possibly avoid potential risks. "Electronic identification, along with geofencing, further aid in addressing security risks by helping to identify potential threats and categorizing zones as particularly sensitive or off-limits. Finally, the enforcement of privacy rights are aided by electronic identification and by using geofencing to make certain zones privacy-focused. Registration, electronic identification, and geofencing are also particularly important for and are constituent elements of unmanned aircraft traffic management , otherwise known as the "U-Space" framework".[154]

The use of drones which include particular features such as sensors and cameras could, through improper or malicious use – either with or without intent-, lead to risks with respect to privacy, surveillance, discrimination and stigmatization. Improper or malicious use could further cause security or safety

[147] Art. 132 Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No. 2111/2005, (EC) No. 1008/2008, (EU) No. 996/2010, (EU) No. 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No. 552/2004 and (EC) No. 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No. 3922/91 Preamble para 28.

[148] Art. 25 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) (Text with EEA relevance)

[149] Ibid.

[150] Annex IX, point 1.3, of the Regulation (EU) 2018/1139

[151] Eleonora, B. (2020). From here to 2023: Civil drones operations and the setting of new legal rules for the european single sky. *Journal of Intelligent & Robotic Systems,* 100(2), 493-503. doi:10.1007/s10846-020-01185-1, p. 499 - 500

[152] Ibid., p. 500

[153] Notice of Proposed Amendment 2017-05 (A), https://www.easa.europa.eu/sites/default/files/dfu/NPA%202017-05%20%28A%29_0.pdf, pg. 6("NPA-A")

[154] ALADDIN [Project 740859], D3.1 – Data protection, Social, Ethical and Legal Frameworks, p. 34

threats. The SOCIO BEE project should invest significantly in safety, security and compliance to avert such external or inside threats.[155] Drones, depending on the equipment they carry, can interfere with the rights to privacy and data protection and even lead to unlawful surveillance. A notable passage in relation to cameras was the distinction between drones and toy drones. "A toy is a product designed or intended (whether or not exclusively) for use in play by children under 14 years of age".[156] Thus as stated in Regulation (EU) 2019/947: "considering the risks to privacy and protection of personal data, operators of unmanned aircraft should be registered if they operate an unmanned aircraft which is equipped with a sensor able to capture personal data. However, this should not be the case when the unmanned aircraft is considered to be a toy within the meaning of Directive 2009/48/EC of the European Parliament and of the Council on the safety of toys".[157]

Member States can either set a different (higher) minimum age, thus affecting this exception.

3.4.4 Future developments to keep an eye on

It will be interesting to see how the transitional phase will evolve and whether the previous fragmentation will not hinder the harmonized implementation.

3.5 The national framework

What follows are the national frameworks of Belgium, Greece, Italy and Spain for drones.[158]

3.5.1 Belgium

3.5.1.1 Key regulator

Agencies Responsible for regulating drones in Belgium:

- Federal Public Service Mobility & Transport (FPS)

3.5.1.2 Relevant framework

The concrete implementation for Belgium as regards Regulation 2019/947 is done by the Royal Decree of 8 November 2020.[159]

3.5.1.3 UAS-Zones and other restrictions

The 'UAS zones' are defined in Belgium by the Ministerial Decree of 21 December 2020.[160]

In Belgium, the website of Droneguide gives an overview of the Belgian airspace that is relevant for drone operators.[161] Here the user can search for specific addresses and/or search on the map. The geozones are also shown for the selected location as determined by the Belgian Directorate General of Aeronautics. The conditions to be met can be verified in the 'Access conditions' tab.

Getting acces to an UAS zone

[155] Call: H2020-LC-GD-2020: SOCIO-BEE, GA No: 101037648, p. 81
[156] Ibid.
[157] EASA, 'Cover Regulation to Implementing Regulation (EU) 2019/947', p. 17
[158] A list of drone website references by country, as supplied by the respective National Aviation Authority (NAA) can be found on https://www.easa.europa.eu/domains/civil-drones/naa
[159] 8 NOVEMBER 2020. - Koninklijk besluit tot uitvoering van uitvoeringsverordening (EU) 2019/947 van de Commissie van 24 mei 2019 inzake de regels en procedures voor de exploitatie van onbemande luchtvaartuigen [Dutch]
[160] 21 DECEMBER 2020. - Ministerieel besluit tot vaststelling van vaste geografische UAS-zones en toegangsvoorwaarden voor vaste geografische UAS-zones [Dutch]
[161] Droneguide, Available: https://map.droneguide.be]

Belgium uses SkeyDrone's Drone Service Application to request access to UAS zones.[162] The user can use two tools: the DSA Planner and the DSA Fly. The former allows you to plan your operation in advance. The latter is needed on the day of your operation.

Use DSA FLY on your smartphone / tablet to request tactical authorization, to indicate you are airborne or have landed and finally, when you are finished, to close your operation.

There are several controlled airspaces around the airports in Belgium of:

- Ostend
- Antwerp
- Brussels
- Charleroi
- Liege
- and the zones around the airport of Kortrijk-Wevelgem

3.5.1.4 Registration and authorization

Registration

The minimum age for pilots differs per category. For 'open A1/A3' the minimum age is 14 years. For 'open A2 and Specific' the minimum age is 16 years. This means that every drone operator has be registered.

Insurance

In Belgium, lighter drones [see: mass of less than 20kg], are also obliged to take out insurance. According to the Royal Decree implementing Regulation 2019/947[163], as laid down in Article 12 of the Royal Decree 2020, every UAS operator in Belgium who exclusively operates flights in the Open category is required to take out civil liability insurance to cover all bodily harm and material damage to third parties. The Belgian regulator warns users that some insurance companies impose restrictions on the conditions for operating a UAV in their exclusion clauses (weight, height, etc.).[164]

3.5.2 Greece

3.5.2.1 Key regulator(s)

Agencies Responsible for regulating drones in the Hellenic Republic (Greece):

- Hellenic Civil Aviation Authority

3.5.2.2 UAS-Zones and other restrictions

No-fly zones and permissions can be checked at the application *Drone Aware.*

Drone Aware - GR (DAGR) is a real-time UAS (drone) information system for Greece developed by the Hellenic Civil Aviation Authority. DAGR provides situational awareness to UAS pilots and operators by informing them about flight limitations and letting them submit flight requests. The system provides

[162] Drone Service Application, Available: https://www.skeyes.be/en/services/drone-home-page/you-and-your-drone/drone-service-application/

[163] 8 NOVEMBER 2020. - Koninklijk besluit tot uitvoering van uitvoeringsverordening (EU) 2019/947 van de Commissie van 24 mei 2019 inzake de regels en procedures voor de exploitatie van onbemande luchtvaartuigen. Available: http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=nl&la=N&cn=2020110802&table_name=wet

[164] Webpage exists only in Dutch or French.

additional resources concerning the acceptance or the rejection of a flight request, aeronautical data and other relevant information.[165]

The flight request and other information can be found on the following webpage:

- http://www.ypa.gr/en/HCAA_UAS_FLT_request_editable.pdf

3.5.2.3 Registration and authorization

To register drones you have to go to web application of Hellenic Civil Aviation Authority.[166] Third party liability insurance is required for any drone a) used for business purposes and b) equal to or over 4 kgs for private use, under national legislation.

3.1.1. Other partner countries

3.5.2.4 Italy

The agency responsible for regulating drones in Italy:

- Ente Nazionale per l'Aviazione Civile

To register drones you have to go to D-Flight portal.[167] The Data Protection Authority of Italy issued a set of recommendations on how to use drones with respect to privacy.[168]

3.5.2.5 Spain

The agency responsible for regulating drones in Spain:

- Agencia Estatal de Seguridad Aérea

The Spanish Data Protection Authority has issued specific guidelines for the use of drones. Those guidelines are presented at the section about the preliminary recommendations. Moreover, the authority had to deal with a number of cases relating to drones. One of them is about a local municipality which did not complete its data protection impact assessment with respect to the use of drones with cameras for traffic monitoring, because the municipality considered that the risk for data subjects would be "acceptable". The authority in this case did not find the municipality in violation of GDPR.[169]

3.6 Specific considerations: children and elderly persons

In EU, users over 16 can register as drone operators. Local aviation authorities may lower the age minimum. A parent/guardian can register the drone for those who are under 16 years old and provide parental or guardian guidance.[170] Moreover, drones when used by children could be considered toys. Products designed or intended whether or not exclusively, for use in play by children under 14 years old should be considered as a toy. In that case, the drones would have to also comply with the Directive 2009/48/EC on the safety of toys.[171]Manufacturers may clearly exclude their product from the application

[165] https://dagr.hcaa.gr/
[166] https://uas.hcaa.gr/Account/Login?ReturnUrl=%2F
[167] https://www.d-flight.it/new_portal/en/
[168] GPDP, 'Consigli per rispettare la PRIVACY se si usa un DRONE a fini ricreativi', 2021, September. https://www.garanteprivacy.it/documents/10160/0/Utilizzo+di+droni+a+fini+ricreativi+e+privacy_+l%27infografica+del+Garante.pdf/482c901c-acc1-4aeb-9a9a-556376f84156?version=2.0
[169] You can find an English translation of the case here: https://gdprhub.eu/index.php?title=AEPD_-_E/02666/2020
[170] More information on the age requirements: https://www.easa.europa.eu/the-agency/faqs/drones-uas
[171] For more information: https://www.easa.europa.eu/faq/119218

of the Directive on the safety of toys (when a confusion is possible) by indicating clearly a minimum age > 13 years on their product (packaging, manual etc.) (e.g; "not for use under 14 years").[172]

The researchers in SOCIO-BEE will ensure that all equipment provided to children is child-proof (based on EU safety standards) and age-appropriate. The children will be briefed in detail about the proper use of the drones before these are used. Especially for research involving children who are unable to make decisions for themselves, entails that researchers must maintain an active relationship with their legal guardians and/or carers. This means that the legal guardians must be allowed to monitor the activities and be in continuous communication with the researchers. Thus, all activities involving children will take place in controlled environments.
Concerning the research involving elderly people and aged populations, elderly persons are considered an important target group of the project, provided that its tools and equipment will be designed to be used by people of different ages and skills (for example user-friendly interfaces, easy mechanisms for data capturing and processing, simple procedures for registering in the programs offered by the platform). The SOCIO-BEE will engage elderly persons over 65 years old and whenever necessary caretakers

3.7 Preliminary recommendations

3.7.1 European Union Aviation Safety Agency

EASA has published clear guidelines on drones of different Cx labels within the open category on its website.[173] The do's and don'ts for each class are briefly and visually summarised.

An example of a drone, class C0 with camera:

[172] EASA, 'When is a drone considered to be a toy?', Available at: https://www.easa.europa.eu/faq/119218
[173] EASA, 'Drones Information Notices', [Online]. Available : https://www.easa.europa.eu/document-library/general-publications/drones-information-notices

Figure 5. EASA Drones Information Notices

3.7.2 Important steps for Open Category

Before a flight can be performed, it is important to follow the following steps:

1. Start identifying what type of drone it is: is it still an old model or does it already have a Cx label? [taking into account the exceptions with the transitional period]
2. Plan your route
3. Check overlap between your flightplan and any GeoZone and if so: comply with all relevant GeoZone rules, including eventual need to get flight authorization from the GeoZone manager

3.7.3 Guidelines with respect to data protection and privacy concerns

There are several manuals and tips to better deal with privacy and data protection risks. The project DroneRules.eu, co-funded by the COSME programme of the European Union, has released two documents to better deal with the aforementioned risks. The Privacy Handbook is an "easy to read guide about key privacy and data protection risks that arise when you are operating drones for recreational purposes" [174] . Although the distinction between recreational and professional drones no longer applies with the new regulation of 2019, it still contains good information and suggestions.

Finally, lists of recommendations have also been adopted to some national supervisors such as the Information Comissioner's Office[175] and the Spanish Data Protection Authority[176].

Those lists, considering the potential intrusions to privacy, require drone operators to:

[174] DroneRules.eu, 'Privacy Handbook', [Online]. Available: https://dronerules.eu/assets/handbooks/PrivacyHandbook_EN.pdf, p. 1
[175] UK Information Commissioner's Office, 'Drones'. [Online]. Available: https://ico.org.uk/your-data-matters/drones/
[176] Agencia Española de Protección de Datos, 'Drones and
Data Protection'. 2019, [Online]. Available: https://www.aepd.es/sites/default/files/2019-09/guia-drones.pdf.

- Inform about the use of drones with embedded cameras and sensors before their actual use
- To thoroughly consider the surroundings and avoid private and restricted areas
- To check the camera's and sensors' capacity and install equipment in a way that would not lead To the unique identification of an individual (based on resolution, precision, angle of recording)
- To plan ahead a flight itinerary
- To make sure that the drone is always visible and not hidden
- To keep images and other files of collected data securely stored

3.7.4 Safety guidelines

The SOCIO-BEE drone operators will be instructed to follow the necessary safety rules (recommended range and duration of flights, which are the proper weather conditions for a flight, what is the recommended distance from humans and animals, how to handle a system failure, how to avoid a collision, etc.), including taking into account ways to avoid causing disturbance to their surroundings, e.g., residential regions, the flora and the fauna of an area as well as the ecosystem of a natural zone. [177]

For the use of drones, the consortium will consult the applicable regulation of the countries where the drones will be tested and will set an operational framework. The use of the drones should primarily respect the rules of the national civil aviation authorities. The partners in charge of the drones will program the drones in such a manner that several rules will be applied by default (e,g., drones cannot go further or higher than programmed). Again, both researchers and research participants will be briefed about the boundaries of use and will be bound to a particular framework of operation. A liability and insurance scheme will be in place to safeguard from any damages. [178]

Drones improperly used can pose serious security risks. A main security drawback is that they are vulnerable to malicious and criminal misuse, cyber-attacks and can be used purposefully or accidentally erroneously by an insider. For that reason, specific security safeguards will be outlined and implemented in the Data Management Plan in line with European Union Agency for Cybersecurity (ENISA)'s Paper 'Towards a framework for policy development in cybersecurity - Security and privacy considerations in autonomous agents'.[179] This includes securing drones against hacking due to their unencrypted communications through radio, WiFi or GPS and proving the quality of a drone's software with verifiable evidence that the system is safeguarded with the baseline security principles.[180]

[177]Call: H2020-LC-GD-2020: SOCIO-BEE, GA No: 101037648, p. 82-83
[178] Ibid.
[179] EU Agency for Cybersecurity (ENISA), 'Towards a Framework for Policy Development in Cybersecurity -Security and Privacy Considerations in Autonomous Agents'. 2018, [Online]. Available: https://www.enisa.europa.eu/publications/considerationsin-autonomous-agents.
[180]Call: H2020-LC-GD-2020: SOCIO-BEE, GA No: 101037648, p. 82-83

4 Use of wearables in the Socio Bee context: Legal and regulatory framework

4.1 Definition of wearables

4.1.1 Technical definition

Technological devices which consist of electronics, software and sensors and are designed to be worn on the body, are called 'wearables'. However with the rise of data collection and transmission capabilities, they can be defined as "miniaturised computer and sensor devices, which are worn effortlessly on … the body of the wearer" and collect data on the person wearing the device and/or its environment".[181]

Wearables are mostly distinguished from smartphones because they are designed to be hands-free which allow the user to be focused on the task they are doing.[182] Smartphones[183] are not usually classified as wearable technologies despite being among the IoT devices, their portability and their almost ubiquitous presence in close proximity to humans but "many wearables, such as smart watches, are compatible with and can be connected to smartphones".[184]

Wearables, depending on their construction, can collect a variety of data. They often generates large amounts of data with a short amount of time but because they are usually compact, they don't have the capacity to store all the generated data. Therefore they are usually connected online with cloud computing platforms and relying on new technologies and approaches such as Big Data (technologies) that transmit, store and analyse these large and complex amounts of data.[185] The underpinning technology of wearables usually involve one of the follow technologies: "radio-frequency identification, magnetic field, Bluetooth, ultrasonic, laser, video and static camera, global positing system (GPS), the Global Navigation Satellite System, electrocardiogram, sensors and more".[186] SOCIO-BEE will use new low-cost wearable modular sensor devices for air quality monitoring. Sensors are often needed with wearables so that they can detect, among other things, the location or activity of the wearer.

However, it remains difficult to precisely define wearables due to the constant developments within this growing industry.

4.1.2 Legal definition

There is no legal definition of 'wearables' in the European Union, but in December 2016 the Commission published the Smart Wearables reflection and orientation paper where it proposed a definition of smart wearables. In it, the Commission defined wearables as follows: "smart wearables are body-borne computational and sensory devices which can sense the person who wears them and/or their environment. Wearables can communicate either directly through embedded wireless connectivity or through another device (e.g. a smartphone). (…) Smart wearables may have control, communication,

[181] Eurofound, 'Wearable devices: Implications of game-changing technologies in services in Europe', p. 1; Bauer et al, 2016; p. 531; Huang P. Promoting Wearable Computing. In: Jin Q, Li J, Zhang N, Cheng J, Yu C, Noguchi S, editors. *Enabling Society with Information Technology*. Tokyo: Springer Japan; 2002. p. 367-76 .

[182] Bauer, D., Wutzke, R., & Bauernhansl, T. (2016). Wear@Work – A New Approach for Data Acquisition Using Wearables. *Procedia CIRP*. 50. 529-534. doi:10.1016/j.procir.2016.04.121.

[183] The smartphone also comes with challenges in terms of surveillance, cybersecurity, privacy, etc. This is not applicable to this deliverable, as it will be covered in more detail in other deliverables.

[184] Eurofound, WORKING PAPER, Wearable devices: Implications of game-changing technologies in services in Europe, p. 7

[185] Bauer, D., Wutzke, R., & Bauernhansl, T. (2016). Wear@Work – A New Approach for Data Acquisition Using Wearables. *Procedia CIRP*. 50. 529-534. doi:10.1016/j.procir.2016.04.121.

[186] Eurofound, 'Wearable devices: Implications of game-changing technologies in services in Europe', p. 7

storage and actuation capabilities".[187] The definition of 'wearables' therefore has a broad scope that includes many items and technologies.

4.1.3 Internet of Things

Wearables are part of the so called Internet of Things, which can be described as a phenomenon where there is an increasingly embedded connectivity among a plethora of devices.[188] "The IoT can be regarded as an extension of today's internet, the value of which can only be truly recognised if different applications and devices work together seamlessly across and within different sectors, creating system-wide effects and enabling new capabilities and processes".[189]

Low-cost IoT-based sensing

Low-cost IoT sensors differ from other wearables in that they allow interaction with the physical world using wireless communication and computers. They can, for example, monitor air quality. [190]

4.2 Definition of wearables in Socio Bee

The wearable device will include a mobile App (Android) to relay real time data of the wearable to Bettair platform. In this early stage of the project, it isn't clear if there will also be a iOS application.

The wearable/portable devices include:

- State-of-the-art pre-calibrated environmental sensors based on highly sensitive electrochemical cells. NO2 and O3
- Quality control of electrochemical cells to guarantee maximum repeatibility of the electrochemical cells.
- Laser occlusion-based particle matter size and mass determination (PM2.5).
- Corresponding low-noise Analog Front-End
- High-accuracy environmental sensors
- Low-weight device (below 100 g)
- Low energy electronics
- Communications module with Bluetooth 5.X to the users mobile.

Mobile App (Android) to relay real time data of the wearable to Bettair platform.

- Cloud data upload.
- REST API access access air pollution data in Bettair platform.
- Android app with tech: Flutter, React Native, Native Android:
    - **Flutter**: It is a cross-platform framework for the Dart language, it is one of the fastest-growing frameworks that allow the development of mobile (Android, iOS), desktop, and web applications. It is maintained by Google and has a large and growing number of code library packages that facilitate application development.
    - **React Native**: It is a cross-platform framework for the JavaScript language that allows the development of mobile applications (Android, iOS). It is maintained by Facebook and used by large companies (Pinterest, Tesla, Uber eats, etc.). The main advantage over Flutter is

[187] European Commission, 'Smart Wearables Reflection and Orientation Paper', December 2017, p. 4
[188] Evans, D. (2011), The Internet of Things: How the next evolution of the internet is changing everything, white paper 2, Cisco, San Jose, CA, available at http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf
[189] Eurofound; 'Implications of game-changing technologies in the services sector in Europe: Wearable devices', p. 12
[190] Zakaria, N.A.; Abidin, Z.Z.; Harum, N.; Hau, L.C.; Ali, N.S.; Jafar, F.A. Wireless Internet of Things-Based Air Quality Device for Smart Pollution Monitoring. *Int. J. Adv. Comput. Sci. Appl*. 2018, p. 9

that it has been on the market for longer, so it is in a very mature state and has a large community of developers.

- **Native Android:** The Android SDK allows the development of mobile applications using the Kotlin or Java language (even both in the same application). With native apps, you can have total control over the available resources in Android devices. The new Jetpack libraries together with Kotlin coroutines have significantly improved the quality of native application development.

No personal data should be collected by design, at no point the location of a node, and the data measurements it provides is associated with a particular individual, **except** through the particular mobile data interface of the user mobile phone which shall be filtered out at the cloud input interface. The node will include the possibility of encrypting data transmission in order to provide an additional layer of user and IP protection as needed by the project contributors. Data will be geolocalized. (drones and wearables). Finally, an e-mail address (personal data) would be needed to for support. Bettair platform is GDPR compliant.

4.3 The international framework

4.3.1 UN

The United Nations recognises that wearables can help achieve its Sustainable Development goals. An example of this is UNICEF's 2015 'Wearables for Good' challenge which showcased a variety of applications with important humanitarian purposes. Wearables would be designed in a different way that, for example, can alert people with different needs who would otherwise be more difficult to track. Many of these wearables could be used in refugee camps or remote areas that are far from major infrastructure or medical facilities. UNICEF also released a handbook in 2017 that "aims to bring together the design, technology, and social impact communities to encourage the creation of wearable solutions for social good".[191] In relation to this, there are Internet of Things for Development projects.[192] It uses low-cost IoT to make progress in various sectors in developing countries.

4.3.2 Other international bodies/organisations

In the US, the Food and Drug Authorities (FDA) have drawn up a regulatory initiative for wearables.[193]

4.4 The EU framework

4.4.1 Historical developments

An important event for EU was the Information and Stakeholders' Day on Wearables in December 2015 by the European Commission [DG Connect] where different EU stakeholders discussed major technology advances, applications and market issues to identify progress, barriers and opportunities for Europe. In 2016 the Commission published the paper 'A reflection and orientation paper on smart wearables' which collected a variety of contributions from EU stakeholders. It "raised some important questions in the Smart Wearables domain (e.g. related to testing, standardisation and data protection) and offered suggestions for actions needed to support further technology development, innovation and

[191] See: https://www.unicef.org/innovation/reports/wearables-good-challenge-use-case-handbook
[192] Internet of Things for Developing Countries, See: https://team.inria.fr/iot4dc/
[193] https://www.fda.gov/regulatory-information/search-fda-guidance-documents/general-wellness-policy-low-risk-devices

deployment".[194] Since then, the Commission has taken several steps towards a coordinated policy for Smart Wearables in EU.

4.4.2 Current and applicable framework

An important step was taken in Horizon 2020. In the 2018-2020 work programme, wearables are given a prominent role in the ICT programme 'Information and Communication Technologies'.[195] This programme further develops the digitalisation of European industry and services.

Wearables are specifically discussed in proposal' ICT-02-18: Flexible and Wearable Electronics'. In it, the European Commission formulates the specific challenges of Wearables as follows: "Flexible and Wearable Electronics combines new and traditional materials with large-area processes to fabricate lightweight, flexible, printed and multi-functional electronic products. The challenge is to tap open opportunities in existing and emerging markets by pushing technology barriers further and demonstrating innovative use in sectors that could benefit from such innovations".[196]

The Commission recognises that there are technological and non-technological barriers associated with wearables that may limit the innovation capacity of European industry. The EU is seeking to address these barriers through increased research and development efforts.[197] A major sticking point is the development of an appropriate regulatory framework, which had already been confirmed at the Stakeholders Day on Wearables in 2015. For example, the Commission states that "a clear regulatory framework providing at the same time freedom-to-innovate and ensuring an appropriate level of protection for users' health, safety, data and privacy is needed. The most important areas concerned are data protection, data privacy, free flow of data, liability and consumer protection (e.g. in the field of medical devices)".

4.4.2.1 Privacy and data protection law

General

The potential privacy, data protection and security implications of wearables remain problematic and challenging as they often generate and collect a lot of personal data of a potentially sensitive nature such as location, age, gender, preferences or behaviour. This also involves various risks of which a wearer should be aware. Due to their design, (a large part of) the data generated by wearables will often be collected and stored by the device manufacturer or a third party, which makes the situation paradoxical for the user. The user owns the device, but not the data. This data can therefore be sold on (by consent) to third parties.[198] Although this data can also be anonymised, there is still a chance of a breach of this privacy protection measure. For example, algorithms have the capacity to compare data sources via digital traces of users and recent "research suggests that such approaches can be remarkably accurate in approximating and collating personal data (see, for example, Lambiotte and Kosinski, 2015)". Furthermore, platforms where the data is stored can suffer from cyberattacks, which can result in the loss of much valuable and sensitive information.

[194] European Commission, 'Smart Wearables Reflection and Orientation Paper – Including Feedback from Stakeholders, https://digital-strategy.ec.europa.eu/en/news/feedback-stakeholders-smart-wearables-reflection-and-orientation-paper
[195] European Commission, 'Horizon 2020 – Work Programme 2018-2020, Information and Communication Technologies', Avaible: https://ec.europa.eu/research/participants/data/ref/h2020/wp/2018-2020/main/h2020-wp1820-leit-ict_en.pdf
[196] Ibid., p. 31
[197] European Commission, 'Smart Wearables Reflection and Orientation Paper – Including Feedback from Stakeholders, https://digital-strategy.ec.europa.eu/en/news/feedback-stakeholders-smart-wearables-reflection-and-orientation-paper, p. 17
[198] Piwek, L., Ellis, D. A., Andrews, S. and Joinson, A. (2016), The rise of consumer health wearables: Promises and barriers, *PLoS Med*, Vol. 13, No. 2, pp. e1001953, available at https://doi.org/10.1371/journal.pmed.1001953.

Specifically for wearables, the connection between the wearable and the rest of the IoT or, for example, smartphones, may also be subject to breaches. The security of the communication technology may therefore have weaknesses. Depending on the level of encryption, this security may or may not be secure. A widely used technology such as Bluetooth is known for its low level of encryption.[199] The wearables can also be lost or stolen, and if they contain sensitive data, this must be protected. [200]

A main security drawback is therefore that they are vulnerable to malicious and criminal misuse, cyber-attacks and can be used purposefully or accidentally erroneously by an insider. For that reason, specific security safeguards will be outlined and implemented in the Data Management Plan in line with ENISA's Paper 'Towards a framework for policy development in cybersecurity - Security and privacy considerations in autonomous agents' [22]. This includes securing wearables against hacking due to their unencrypted communications through radio, WiFi or GPS and proving the quality of a drone's software with verifiable evidence that the system is safeguarded with the baseline security principles.[201]

Legal protection

GDPR and the e-Privacy Directive

The existing European regulatory framework offers privacy and data protection in the collection and processing of personal data from wearables today. As with Drones, primary and secondary EU legislation applies here too. "The protection of personal data is to be found in the EU Charter for the protection of Fundamental Rights and Freedoms (EUCFR) (Article 8), and in Article 16 TFEU and Article 39 of the TEU. The right to data protection at EU level is further specified in the secondary legislation. In particular, with respect to SOCIO-BEE the main regulation would include:

- the General Data Protection Regulation and the implementing national acts
- the e-Privacy Directive and the transposing national acts[202]

The e-privacy directive "harmonises the provisions of the Member States required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the Community".[203] The legislation thus guarantees the right to privacy when using wearables, mobile phones, surfing the Internet or other Internet-connected devices.

Data generated and interpreted by sensors of the wearables are therefore of a digital nature and therefore subject to strict control from the moment this data is obtained. "E.g.: (…) the use of remote sensing[204] technologies in the current era may interfere with the rights to informational and location privacy.

[199] Thierer, Adam A. D. (2014), 'The Internet of Things and wearable technology: Addressing privacy and security concerns without derailing innovation.', Richmond Journal of Law & Technology, Vol. 21 (2014), p. 1.
[200] Wei, Jh. 'How wearables intersect with the cloud and the Internet of Things: Considerations for the developers of wearables', *IEEE Consumer Electronics Magazine*, Vol. 3, No. 3, pp. 53–56.
[201] Call: H2020-LC-GD-2020: SOCIO-BEE, GA No: 101037648, p. 82-83
[202] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002, p. 37–47
[203] Electronic Privacy Information Center, 'EU Privacy and Electronic Communications (e-Privacy Directive)'. Available at : https://archive.epic.org/international/eu_privacy_and_electronic_comm.html
[204] "Remote sensing may be broadly defined as the collection of information about an object without being in physical contact with the object. Aircraft and satellites are the common platforms from which remote sensing observations are made. The term remote sensing is restricted to methods that employ electromagnetic energy as the means of detecting and measuring target characteristics." Sabins, F. Floyd. 1978. *Remote Sensing: Principles and Interpretation*. San Francisco: W. H. Freeman

Observation of private spaces with remote sensing technologies or the location of a person (even without collection of data) or even the correlation of collected data with other data may reveal information about individuals' (private) life".[205]

It is possible with wearables that sensitive personal data is being processed. If this is the case, then this data falls under the category of "special category data" as stated by the GDPR and requires more protection because of its nature.[206] Therefore it is also possible that explicit consent of the citizen scientist will be required to process this type of data. It is important that this consent must be freely given, specific and informed and are an unambiguous indication of the user's wishes. For the processing of sensitive data, consent must be given in words therefore consent through the use of the wearables will not be sufficient.

Cybersecurity Act

In 2019, the Cybersecurity Act[207] went into effect. This new regulatory framework consists of several measures to better deal with cyber-attacks and to build a strong cyber-security in Europe. The act consists of two main frameworks, namely:

- Strengthening the role of ENISA
- Creating an European framework for cybersecurity certification

ENISA will become a permanent agency and will be given more resources and tasks, one of which will be the key role in establishing and maintaining the European cyber security certification system for ICT products, processes and services in the EU. This also includes improving the security of, among other things, 'IoT devices'. It "incorporates security features in the early stages of their technical design and development (security by design). It also enables their users to ascertain the level of security assurance, and ensures that these security features are independently verified".[208] It therefore contains a comprehensive set of regulations, technical requirements, standards and procedures. Companies will only have to apply once for the entire EU market.

This system is one of the measures in the broad cybersecurity package proposed by the Commission in 2018 as part of the Digital Single Market.[209]

Cybersecurity Strategy 2020

In 2020, the EC together with the High Representative of the Union for Foreign Affairs and Security Policy proposed the new EU Cybersecurity Strategy, which will serve as a key component of Shaping Europe's Digital Future, the Recovery Plan for Europe and the EU Security Union Strategy. "The Strategy will bolster

[205] Maniadaki, M., Papathanasopoulos, A., Mitrou, L., & Efpraxia-Aithra Maria. (2021). Reconciling remote sensing technologies with personal data and privacy protection in the european union: Recent developments in greek legislation and application perspectives in environmental law. *Laws*, 10(2), 33. doi:10.3390/laws10020033, p. 3

[206] The lawful basis under Article 6 and Article 9 of the GDPR must be identified.

[207] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance), OJ L 151, 7.6.2019, p. 15–69

[208] EU Monitor, 'Cybersecurity Act', Available at : https://www.eumonitor.nl/9353000/1/j9vvik7m1c3gyxp/vku7ds3xlvzx?ctx=vh6tfw7n7epz

[209] European Commission, 'Cybersecurity certification strategy', Available : https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-certification-framework

Europe's collective resilience against cyber threats and help to ensure that all citizens and businesses can fully benefit from trustworthy and reliable services and digital tools".[210]

For this Strategy, there are two new proposals from the EC to address both the cyber and physical resilience of critical entities and networks:

- Directive on measures for high common level of cybersecurity across the Union (NIS 2 Directive)[211]:
    - The previous directive dates back to 2016 and had to be transposed into national law by May 2018. "The directive lays down requirements regarding national cybersecurity capabilities of Member States; rules for their cross-border cooperation; and requirements regarding national supervision of operators of essential services and key digital service providers".[212] The new directive revises the previous one by broadening its scope and "will cover medium and large entities from more sectors based on their criticality for the economy and society. NIS 2 strengthens security requirements imposed on the companies, addresses security of supply chains and supplier relationships, streamlines reporting obligations, introduces more stringent supervisory measures for national authorities, stricter enforcement requirements and aims at harmonising sanctions regimes across Member States. The NIS 2 proposal will help increase information sharing and cooperation on cyber crisis management at national and EU level."[213]
- Critical Entities Resilience (CER) Directive[214]:
    - This directive will expand the scope and depth of the previous related European Critical Infrastructure Directive of 2008 by covering more sectors and obliging Member States to adopt a national strategy to ensure the resilience of critical entities and to carry out regular risk assessments.

Commission Delegated Regulation (EU) 2022/30 to the Radio Equipment Directive

The Radio Equipment Directive 2014/53/EU[215] (RED) set up a regulatory framework for placing radio equipment on the market. "It ensures a single market for radio equipment by setting essential requirements for safety and health, electromagnetic compatibility, and the efficient use of the radio spectrum. It also provides the basis for further regulation governing some additional aspects. These include technical features for the protection of privacy, personal data and against fraud. Furthermore, additional aspects cover interoperability, access to emergency services, and compliance regarding the combination of radio equipment and software".[216]

[210] European Commission, 'New EU Cybersecurity Strategy', [Press Release], Available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2391
[211] Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, COM/2020/823 final
[212] European Parliament, 'Review of the Directive of Network and Information Systems', Available at: https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-review-of-the-nis-directive
[213] European Commission, 'New EU Cybersecurity Strategy', Available at : https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2391
[214] Proposal for a Directive of the European Parliament and the Council on the resilience of critical entities, COM/2020/829 final
[215] Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC Text with EEA relevance, OJ L 153, 22.5.2014, p. 62–106
[216] European Commission, 'Radio Equipment Directive (RED)', Available at: https://ec.europa.eu/growth/sectors/electrical-and-electronic-engineering-industries-eei/radio-equipment-directive-red_en

Due to a growing number of IoT devices, the Commission has recently taken action to improve the cyber security of these wireless devices available on the European market. Following up on the EU Cybersecurity Strategy of 2020, the EC adopted the Delegated Act 2022/30 to the Radio Equipment Directive[217]. This "contains new legal requirements for cybersecurity safeguards, which manufacturers will need to take into account in the design and production of relevant products".[218] It also seeks to raise the level of cybersecurity, personal data protection and privacy. As a result, the EC seeks to make all wireless devices secure before they reach the European market.

This delegated act will enter into force in early 2022 unless the Council and Parliament object. After this, manufacturers will have 30 months to adapt to the new obligations. The legal requirements are expected to apply in mid-2024.

SOCIO-BEE

The use of sensors within Wearables can raise privacy and data security issues. It raises concern about the way air quality sensors (wearables) communicate with e.g. smartphones as they might use IP addresses and information about telephones numbers while collecting information about their environment.[219] These type of data is seen as “personal information” as constituted with the GDPR. The use of wearables which include particular features such as sensors and cameras could, through improper or malicious use – either with or without intent-, lead to risks with respect to privacy, surveillance, discrimination and stigmatization. Improper or malicious use could further cause security or safety threats. The SOCIO BEE project will invest significantly in safety, security and compliance to avert such external or inside threats.

The consortium does not envisage the processing of personal data of research participants through wearables. However, it acknowledges the risks to data protection and privacy that wearable devices may entail for their users or others. Wearable devices, as part of the Internet of Things, will in principle fall both under the General Data Protection Regulation (and the national Implementing Acts) and the e-Privacy Directive (and the national transposition acts). It thus commits to take into account the Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, issued by the European Data Protection Board in 2019,[220] ensuring that only the minimum amount of personal data will be collected and the user will be clearly informed about the processing operations. The legal principles of data protection and privacy by design will be translated into architectural and platform specifications by the technical partners. The technical translation will be based upon a data protection modelling framework that can ensure that the data protection and privacy principles will be rooted in the system from scratch.[221]

4.4.2.2 Safety requirements

[217] Commission Delegated Regulation (EU) 2022/30 of 29 October 2021 supplementing Directive 2014/53/EU of the European Parliament and of the Council with regard to the application of the essential requirements referred to in Article 3(3), points (d), (e) and (f), of that Directive (Text with EEA relevance), OJ L 7, 12.1.2022, p. 6–10

[218] European Commission, ‘Commission strengthens cybersecurity of wireless devices’, Available at: https://ec.europa.eu/commission/presscorner/detail/en/IP_21_5634

[219] Finn, R. (n.d.) ‘Privacy and Data Security for IoT – what are the risks in monitoring our environment?’. [Online]. Available: https://www.trilateralresearch.com/privacy-and-data-security-for-iot-what-are-the-risks-in-monitoring-our-environment/; On General Data Protection Regulation Vulnerabilities and Privacy Issues, for Wearable Devices and Fitness Tracking Applications, p. 4

[220] European Data Protection Board, ‘Guidelines 4/2019 on Article 25 Data Protection by Design and by Default’. 2019, [Online]. Available:https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201904_dataprotection_by_design_and_by_defa ult.pdf.

[221] SOCIO-BEE, Proposal number: 101037648, p. 82

Concerning security, the partners follow closely all the relevant developments and in particular, the work of the European Union Cybersecurity Agency. Specifically, the technical partners will take into consideration guidelines and recommendations included among others in: ENISA, Good Practices for Security of IoT - Secure Software Development Lifecycle (November 2019)[222]; Guidelines for securing the Internet of Things – Secure Supply Chain for IoT (November 2020)[223].

Specifically, with respect to wearables: The SOCIO-BEE consortium will ensure that the wearables manufactured, delivered and tested during the project will consist of high-quality hardware and software, that follows the highest EU safety standards in line with the relevant product liability and certification legislation.[224] The consortium will achieve this, by minimising any risks associated to the devices, by using approved materials, by providing secure interfaces and inclusive, accessible and appropriate design, by including manuals for proper use and by keeping a meaningful documentation of technical specifications. The SOCIO-BEE will not use materials that can cause health hazards when in direct contact with the skin or in any other way. All researchers and research participants will receive training in the safe and proper use of the wearables before deployment.[225]

4.4.3 Future developments to keep an eye on

The progress in the domain of wearables devices and relevant applications is expected to accelerate and many novel devices and components can be expected during the forthcoming two or three years. The SOCIO-BEE approach to functional and architectural design will take under consideration such expectations. The consortium will put efforts to ensure that the future development can be easily integrated into the SOCIO-BEE technological base.

In the field of technology, there are many different developments that may have an impact on the technology used within SOCIO-BEE in the coming years:

- E.g. wearable and mobile sensors (portable air quality monitoring nodes)
  - IoT-based systems
- E.g. Urban air quality monitoring platforms with friendly / accessible / easy to understand information
- High accuracy and methods to assess environmental sensor uncertainty in the wild.
- Portable and wearable AQ multisensor nodes with assessed data quality (indicate measures)
- Platforms that assimilate air quality data with heterogeneous (known) uncertainty and provide end user understable and actionable information.
- Advanced data fusion from heterogeneous sources (open/local data fusion and different sensors and measurement approaches).
- Low-cost HPC upscaling algorithms allow to increase spatial resolution of satellite-based measurements
- Nanomaterial developments to allow to develop ultrathin/ultra”light” wearables.
- New sensor materials.
- Issuing of measurement standards.

[222] ENISA, Good Practices for Security of IoT - Secure Software Development Lifecycle, 2019, [Online]. Available: https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot-1

[223] ENISA, Guidelines for Securing the Internet of Things, 2020, [Online]. Available: https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things

[224] ‘Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety, OJ L 11 p. 4–17’. Jan. 15, 2002, [Online]. Available: https://eur-lex.europa.eu/legalcontent/EN/ALL/?uri=CELEX%3A32001L0095.

[225] SOCIO-BEE, Proposal number: 101037648, p. 81

European Accessibility Act

There are specific products and services on the European single market that are of interest to disabled or elderly people. These products include computers and operating systems, smartphones, access to audio-visual media services, etc. However, the accessibility requirements for these can differ between Member States. Therefore, in order to make this more accessible and harmonised in the European single market, a European Accessibility Act has been created.

The European accessibility directive[226] "aims to improve the functioning of the internal market for accessible products and services, by removing barriers created by divergent rules in Member States".[227]

This directive is part of the 'Strategy for the rights of persons with disabilities 2021-2030' adopted by the EC in 2021.[228] "The objective of this Strategy is to progress towards ensuring that all persons with disabilities in Europe, regardless of their sex, racial or ethnic origin, religion or belief, age or sexual orientation: a) enjoy their human rights; b) have equal opportunities, equal access to participate in society and economy; c) are able to decide where, how and with whom they live; d) move freely in the EU regardless of their support needs; e) no longer experience discrimination (…) in accordance with Article 1 of the United Nations Convention on the Rights of Persons with Disabilities".[229]

Wearables have the potential to positively influence people with disabilities or the elderly. However, the needs of these groups must thus be taken into account.

Cyber Resilience Act

Following up on the EU Cybersecurity Strategy of 2020 and in order to increase the (EU), the European Commission President announced plans for a European Cyber Defence Policy "Including legislation setting common standards under a new European Cyber Resilience Act".[230]

The upcoming Cyber Resilience Act is expected to build on the previous mentioned rules regarding Commission Delegated Regulation (EU) 2022/30 to the Radio Equipment Directive covering more products and looking at their whole life cycle. This regulation therefore also complements the new NIS-Directive

E-privacy regulation

The aforementioned e-Privacy Directive has long been under review so that it can keep up with the speed at which IT-based services and products are evolving, thereby increasing the protection of people's private lives and opening up new opportunities for business in the digital economy. In 2017, the EC approved the proposal for the e-Privacy Regulation. Currently, opinions on the legal procedure have been published by the Economic and Social Committee and the European Data Protection Supervisor. The ePrivacy Regulation is "intended to cover more than just conventional telecommunications services, such as Internet access services, fixed and mobile telephone services or SMS services. Category 1 Over-the-Top services (OTT-I services) such as the messenger and VoIP services WhatsApp, Skype and Threema, e-mail

[226] Directive (EU) 2019/882 of the European Parliament and of the Council of 17 April 2019 on the accessibility requirements for products and services (Text with EEA relevance), *OJ L 151, 7.6.2019, p. 70–115*
[227] European Commission, 'European accessibility act', See: https://ec.europa.eu/social/main.jsp?catId=1202
[228] European Commission, 'Union of Equality - Strategy for the Rights of Persons with Disabilities 2021-2030', Brussels , 3.3.2021 COM(2021) 101 final
[229] European Commission, 'Union of equality: Strategy for the rights of persons with disabilities 2021-2030', See: https://ec.europa.eu/social/main.jsp?catId=1484&langId=en
[230] European Commission, 'How a European Cyber Resilience Act will help protect Europe', [Blog Post], Available at: https://ec.europa.eu/commission/commissioners/2019-2024/breton/blog/how-european-cyber-resilience-act-will-help-protect-europe_en

services such as Gmail and Posteo, and machine-to-machine transmission services (M2M communication services) are also set to fall within the scope of the ePrivacy Regulation".[231]

Debate

However, there have been many debates regarding this regulation. Both internally in the European Council of Ministers as well as during trilogue negotiations between the three institutions (European Commission, European Parliament and EU Council of Ministers) there are discussions on various issues. While Parliament is clearly in favour of the "do not track" standard and is pushing for a consistent requirement for consent, the Council takes the opposite position and calls for more exceptions. If an agreement is reached, the corresponding version would enter into force 20 days after publication in the Official Journal of the European Union after adoption and, as things stand, would apply again 24 months after its entry into force".[232] The e-Privacy Regulation is not expected to enter into force before 2023 and, due to the transitional period of 24 months, will probably not apply before 2025.

Other substantive discussions included the exact scope of the regulation. One example was whether or not pure OTTI-I services are included. Ultimately, these services will be included in the scope due to a recent CJEU ruling of 13 June 2019 (Gmail - C-193/18). [233]

There were also for example debates about the explicit inclusion of M2M communications. For example, the EC judged that these do fall within the scope, but the EP judged that they do not.

4.5 The national framework

4.5.1 Greece

4.5.1.1 The implementation of the Principle of Proportionality in case of conflicting between protected human rights

The SOCIO-BEE project will use sensors for wearables and drones. In Greece, there are some developments that may be relevant in the context of monitoring technologies (e.g. sensors). [234] In case sensors process personal data, there are international, European and national legislations for this, which are implemented by the data protection authority of the respective Member State. [235]

The right to environmental protection[236] as well as the right to personal data, privacy and personal protection are, among others, protective human rights provided by the Greek constitution. [237] In Greece, possible conflicts between such rights are resolved through the implementation of the principle of proportionality. [238] Thus, when a restriction on one of these rights is necessary, appropriate and in stricto

[231] CMS Germany, 'Scope of application of the e-privacy regulation', Available at: https://cms.law/en/deu/insight/e-privacy/scope-of-application-of-the-e-privacy-regulation
[232] CMS Germany, 'ePrivacy Regulation', Available at: https://cms.law/en/deu/insight/e-privacy
[233] CJEU, Google LLC v Bundesrepublik Deutschland (Fourth Chamber) of 13 june 2019, Case C-193/18
[234] Maniadaki, M., Papathanasopoulos, A., Mitrou, L., & Efpraxia-Aithra Maria. (2021). Reconciling remote sensing technologies with personal data and privacy protection in the european union: Recent developments in greek legislation and application perspectives in environmental law. *Laws*, *10*(2), 33. doi:10.3390/laws10020033
[235] Article 9A of the Constitution of Greece: Article 9A: All persons have the right to be protected from the collection, processing and use, especially by electronic means, of their personal data, as specified by law.; regulated by Law 4624/2019; Directive (EU) 2016/680;
[236] Article 24 par. 1 and Article 117 par. 3 of the Constitution of Greece
[237] Articles 9, 9A, 5 of the Constitution of Greece
[238] Article 25 par. 1 of the Constitution of Greece

sensu proportionate, a legal restriction on one of these human rights may be considered if it is necessary in a particular context.

This restriction is subject to special strict rules "because personal data are connected to elements of human personality and in particular the private sphere of the individual".[239] This consideration can thus take place when a project needs to collect personal data in the context of environmental protection. The Data Protection Authority (DPA) of Greece has ruled in two opinions that restrictions on the right to personal data protection can be legally implemented. This includes purposes such as the protection of the environment. [240]

Greek case law also shows that no right is absolute and that restrictions can be made for reasons of public interest in accordance with the criteria imposed by the proportionality principle. [241] This legal limitation of personal data protection is also recognised by the Council of State in line with the DPA's guidelines, "that personal data may only be lawfully taken and processed when a legal interest is to be satisfied, provided that this legal interest obviously outweighs the rights and interests of the personal data subject and only if the legal order does not provide any other way for satisfying the specific legal interest".[242]

For surveillance equipment, the DPA Directive no. 1/2011 in relation to video surveillance systems is also potentially relevant as its Article 5 'the principle of proportionality' provides that the lawfulness of the processing of personal data shall be assessed in accordance with the legitimate aim pursued and the principle of proportionality. [243]

4.6 Specific considerations: children and elderly persons

The children and elderly will be briefed in detail about the proper use of the wearables and the drones before these are used. Children are a special group in the new IoT because they come into contact with various technologies from an early age, either consciously or unconsciously. However, they are often unaware of the many dangers that these IoTs may entail. At an early age, the fundamental rights of this group may therefore already be adversely affected (such as the right to privacy). In the long term, they will be even more exposed to surveillance. It is therefore important to protect this group as much as possible against this. The elderly are also a vulnerable group in this case, since they are often not or no longer up to speed with the rapid developments of these technologies.

4.7 Preliminary recommendations

SOCIO-BEE safety and privacy and data protection guidelines

Specifically, with respect to wearables: The SOCIO-BEE consortium will ensure that the wearables manufactured, delivered and tested during the project will consist of high-quality hardware and software, that follows the highest EU safety standards in line with the relevant product liability and certification

[239] DPA, Opinion 4/2020, Decision 31/2019
[240] DPA, Opinion 2/2010
[241] Hellenic Supreme Court (Plen. Sess.) 1/2017, Hellenic Council of State 1616/2012, 2254/2005.
[242] Maniadaki, M., Papathanasopoulos, A., Mitrou, L., & Efpraxia-Aithra Maria. (2021). Reconciling remote sensing technologies with personal data and privacy protection in the european union: Recent developments in greek legislation and application perspectives in environmental law. *Laws*, *10*(2), 33. doi:10.3390/laws1002003, p. 13 ; Hellenic Council of State 265/2017, 2254/2005.
[243] Maniadaki, M., Papathanasopoulos, A., Mitrou, L., & Efpraxia-Aithra Maria. (2021). Reconciling remote sensing technologies with personal data and privacy protection in the european union: Recent developments in greek legislation and application perspectives in environmental law. *Laws*, *10*(2), 33. doi:10.3390/laws10020033, p. 13

legislation [19]. The consortium will achieve this, by minimising any risks associated to the devices, by using approved materials, by providing secure interfaces and inclusive, accessible and appropriate design, by including manuals for proper use and by keeping a meaningful documentation of technical specifications.

The SOCIO-BEE will not use materials that can cause health hazards when in direct contact with the skin or in any other way. All researchers and research participants will receive training in the safe and proper use of the wearables before deployment.

Concerning security, the consortium aims to avoid security by obscurity and encompasses security by design against inside and external threats. The partners follow closely all the relevant developments and in particular, the work of the European Union Cybersecurity Agency (ENISA). Specifically, the technical partners will take into consideration guidelines and recommendations included among others in: ENISA, Good Practices for Security of IoT - Secure Software Development Lifecycle (19 November 2019).

[…] The legal principles of data protection and privacy by design will be translated into architectural and platform specifications by the technical partners. The technical translation will be based upon a data protection modelling framework that can ensure that the data protection and privacy principles will be rooted in the system from scratch

Guidelines and harmonization standards to the common application of the RED

A guide to the common application of the RED has also been issued. It has no weight in law but deals with practical issues that are of interest to manufacturers and other stakeholders. The guide will be continuously updated, following the discussions and the opinion of the TCAM.

This guide can be found at:

- https://ec.europa.eu/docsroom/documents/33162

Manufacturers of IoT devices must also check that their products comply with EU regulations on safety, health and environmental protection. “It is the manufacturer’s responsibility to carry out the conformity assessment, set up the technical file, issue the EU declaration of conformity, and affix the CE marking to a product. Only then can this product be traded on the EEA market”.[244]

The guide on CE marking for professionals can be found at:

- https://ec.europa.eu/growth/single-market/ce-marking/manufacturers_en

Standardisation

Finally, there are also voluntary harmonised standards in support of the RED that have been and are being prepared by CENELEC and ETSI in reply to the standardisation request M/536[245]

[244] European Commission, ‘Guidance on CE marking for professionals’, Available at: https://ec.europa.eu/growth/single-market/ce-marking/manufacturers_en

[245] M/536 COMMISSION IMPLEMENTING DECISION C(2015) 5376 final of 4.8.2015 on a standardisation request to the European Committee for Electrotechnical Standardisation and to the European Telecommunications Standards Institute as regards radio equipment in support of Directive 2014/53/EU of the European Parliament and of the Council.

5 Use of Artificial Intelligence and Machine Learning: Legal and regulatory framework

5.1 Definition of AI and machine learning

Defining artificial intelligence has some challenges. For example, depending on the field, there are differences between scientific definitions and legal definitions, and even within these there is no consensus. Regulatory and legislative frameworks have only recently been developed and because technology is constantly evolving at a rapid pace, it remains a challenge to capture all these recent developments.[246] In Europe, there is a baseline definition for AI that is supported by the majority of scientific literature. Thus we start from the following definition of Artificial Intelligence (AI), as proposed within the European Commission's Communication on AI[247]:

> *"Artificial intelligence (AI) refers to systems that display intelligent behaviour by analysing their environment and taking actions – with some degree of autonomy – to achieve specific goals. AI-based systems can be purely software-based, acting in the virtual world (e.g. voice assistants, image analysis software, search engines, speech and face recognition systems) or AI can be embedded in hardware devices (e.g. advanced robots, autonomous cars, drones or Internet of Things applications)".*

The Joint Research Centre has also developed an operational definition "based on a taxonomy that maps all the AI subdomains from a political, research and industrial perspective".[248]

However, to ensure better legal certainty, the EC has proposed to define the notion of AI systems more thoroughly. Their definition is crucial in terms of allocating legal responsibilities in the new EU AI framework. In the new AI Act draft, the EC therefore draws up a new legal definition for 'AI systems' specific to European law. This definition[249] is largely based on that of the OEC and is as follows:

> *"[…] software that is developed with [specific] techniques and approaches [listed in Annex 1] and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with".*

Important to note that this article 3(1) also provides a list of definitions "including that of 'provider' and 'user' of AI systems (covering both public and private entities), as well as 'importer' and 'distributor', 'emotion recognition', and 'biometric categorisation'".[250] Annex 1 also defines a list of techniques and approaches used to develop AI.

However, it is important to remember that these previous attempts at defining AI have also attracted criticism from among academics as well as stakeholders involved with the new AI Act. In this way "Smuha and others warn the definition lacks clarity and may lead to legal uncertainty, especially for some systems that would not qualify as AI systems under the draft text, while their use may have an adverse impact on

[246] European Parliament, 'BRIEFING - Artificial intelligence act', PE 698.792 – November 2021
[247] Communication from the Commission to the European Parliament, the European Council , the Council , the European Economic and Social Committee and the Committee of the Regions on Artificial Intelligence for Europe, Brussels ,25.4.2018 COM(2018) 237 final
[248] European Parliament, 'BRIEFING - Artificial intelligence act', PE 698.792 – November 2021, p. 4
[249] Article 3(1) European Commission, 'Proposal for a regulation of the European Parliament and of the council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain Union legislative acts' COM(2021) 206 final
[250] European Parliament, 'BRIEFING - Artificial intelligence act', PE 698.792 – November 2021, p. 4-5

fundamental rights". [251] Among the stakeholders there were also comments about the scope of the definition and the notion of AI systems.[252]

5.2 Definition of AI and machine learning in Socio Bee

The SOCIO-BEE project will introduce and evaluate novel Artificial Intelligence and Machine Learning Algorithms (AI/ML) in order to serve one of its main objectives namely the establishment of an open and sustainable decision-making process with a data analysis platform for the overall CS process: cross-linking of environmental data in collaboration with citizens, scientists, citizen observatories and local decision makers.

To interpret vast amounts of data, it is necessary to provide the various action groups with easy to use and intuitive tools which will allow them to make better actions for improving air quality in the cities. These tools must be able to curate, process and visualize information from various sources, and convert it into value-added information to democratize environmental citizens' action while improving new or existing interventions. To this end we will put efforts to combine seamlessly data processing algorithms and data fusion techniques ready to be used by non tech savvy users. The project aims to develop easy-to-use intelligence and data analytics tools for understanding, curating or validation of data quality and data freshness by action groups.

The above developments rely strongly on novel AI/ML techniques that will be applied in the context of relevant algorithms. In SOCIO-BEE terminology the anticipated tools and components are called collectively "Enablers for Citizen Science" and they will be developed in the frame of WP4. The development, testing and maturation of SOCIO-BEE AI/ML algorithms span over almost all tasks of WP4.

The main functionality of the SOCIO-BEE AI/ML Algorithms rests on three main pillars:

1. Recognition of patterns in vast datasets coming from any kind of air quality sensors that will be engaged in SOCIO-BEE.
2. Personalization of strategy of actions for each user, user group or other local interest groups, by applying AI/ML to optimize the matching between the existing situation and the features and dynamics of each user or group.
3. Visual Analytics with identification of insights and representation in an optimal way through effective web and mobile front-ends

Among others, two iconic examples of AI/ML application in SOCIO-BEE are the following:

a. Micro Volunteering Engine (MVE), integrated with Personalized Messaging and Task engine: The MVE aims to be used by the Working Bees, with the scope of solving the requests allocation problem i.e. the allocation of tasks to available Working Bees or other users to support and provide data for open requests and campaigns existing in the SOCIO-BEE platform
b. Individual Exposure Analytics. This SOCIO-BEE module will collect air pollution concentration values and exposure data for the users. It will work together with behavioural analytics and would be possible to be accessed by an API or by the mobile and web dashboard that SOCIO-BEE develops. The module will track the aggregated exposure of citizens to pollutants and will compute the expected exposition of a route between two locations. It will analyse and correlate,

[251] Ibid., p. 9; Smuha N., and others, *How the EU Can Achieve Legally Trustworthy AI: A Response to the European Commission's Proposal for an Artificial Intelligence Act,* Elsevier, August 2021.
[252] See Ibid., p. 8

using AI/ML algorithms, which activities are more likely to put the user under high air-pollution exposure and which are not. It is important to mention that the AI/ML in SOCIO-BEE will only provide functionality regarding the collection and interpretation of data towards pattern recognition and insights, optimization of strategies and visual analytics. No use of actuators, neither any interaction with such devices is foreseen during the project.

The SOCIO-BEE mobile app will provide several features to the users, including location-sensitive micro-volunteering tasks. AUTH will incorporate and further extend the elements of MoJo-MATE, a mobile journalism application dedicated to manage Crowdsourced/User Generated Content , proposing the so-called Bee-MATE app. The inspired functionality will provide the tools for multimodal data capturing and sharing, leading to richer content and better audience engagement. In this case, end users (working bees) will use smartphone built-in audiovisual equipment, rather than air-pollution measurement equipment. The services running in the back-end will be responsible for processing and analyzing the content captured by the working bees while volunteering. These services will extract context and location-based information from audio, visual, and Global Positioning System input, facilitating environmental sound categorization, event detection and indexing, and their correlation with specific profiles of air pollution management.

Intuitive media user experience will be studied to strengthen ease-of-use, investigating new trends such as sonic and zero interfaces, audiovisual captioning, etc. The crowdsourcing model can lead to more active user involvement and audience engagement, through micro-volunteering tasks and keen communication strategies.

In sum, Bee-MATE will consist of:

- Bee-MATE client: for crowdsourcing, multimodal data acquisition and sharing,
- Bee-MATE server: for post-capturing functionality, for data analysis and semantic annotation of audio and audiovisual crowdsourced content

5.3 The international framework

5.3.1 UN

In 2021, “all the 193 Member states of the UN Educational, Scientific and Cultural Organization (UNESCO) adopted a historic agreement that defines the common values and principles needed to ensure the healthy development of AI”.[253] This Recommendation on the ethics of AI will serve as a basis / guide for further development of legal infrastructures to ensure the ethical development of this technology.

“The text aims to highlight the advantages of AI, while reducing the risks it also entails. According to the agency, it provides a guide to ensure that digital transformations promote human rights and contribute to the achievement of the Sustainable Development Goals, addressing issues around transparency, accountability and privacy, with action-oriented policy chapters on data governance, education, culture, labour, healthcare and the economy”.[254]

5.3.2 Council of Europe

[253] UN, ‘193 countries adopt first-ever global agreement on the Ethics of Artificial Intelligence’, November 25, 2021, Available at: https://news.un.org/en/story/2021/11/1106612
[254] Ibid.

The Ad hoc Committee on Artificial Intelligence (CAHAI) of the CoE is currently working on a legal framework for the development, design and application of AI, based on CoE's standards on human rights, democracy and the rule of law.

The Council of Europe's Committee of Ministers established the mandate for the Ad Hoc Committee on Artificial Intelligence (CAHAI) in 2019. This committee "is charged with examining the feasibility and potential elements of a legal framework for the design, development, and deployment of AI systems that accord with Council of Europe standards across the interrelated areas of human rights, democracy, and the rule of law".[255] In 2020, a Feasibility Study by the CAHAI came out that "examines how the fundamental rights and freedoms that are already codified in international human rights law can be used as the basis for such a legal framework. It proposes nine principles and priorities that are fitted to the novel challenges posed by the design, development, and deployment of AI systems. When codified into law, these principles and priorities create a set of interlocking rights and obligations that will work towards ensuring that the design and use of AI technologies conform to the values of human rights, democracy, and the rule of law". [256]

International legal instruments applicable to AI

There are no international legal instruments specifically addressing the challenges of AI systems to human rights in a comprehensive manner. "There are, however, a number of international legal instruments that partially deal with certain aspects pertaining to AI systems indirectly" found in a recent analysis for CAHAI.[257] "It noted that various international legal instruments already exist to safeguard human rights more generally[258], to safeguard the rights of specific groups in light of vulnerabilities that are also relevant in an AI context[259], and to safeguard specific human rights that can be impacted by AI. The latter encompass, for instance, the right to non-discrimination[260] and the right to the protection of privacy and personal data[261], particularly in the context of automated personal data processing".[262]

Convention 108+ in particular is an important component for transparency and accountability, along with the GDPR. This protocol was amended to modernise it, but is not yet in force.[263] There are also other international legal elements applicable to specific sector[264] or domains indirectly related to AI as well as legal elements for procedural rights. CAHAI believes that these are all relevant, but not always adequate

[255] Leslie, D., Burr, C., Aitken, M., Cowls, J., Katell, M., and Briggs, M. (2021). Artificial intelligence, human rights, democracy, and the rule of law: a primer. The Council of Europe. Available: https://www.turing.ac.uk/research/publications/ai-human-rights-democracy-and-rule-law-primer-prepared-council-europe
[256] Ibid.
[257] Council of Europe, 'Feasibility Study', CAHAI(2020)23. Available: https://rm.coe.int/cahai-2020-23-final-eng-feasibility-study-/1680a0c6da, p. 18
[258] E.g. the European Convention on Human Rights (ETS No. 5) and its Protocols; the European Social Charter (ETS No. 163); the International Bill of Human Rights; and the EU Charter of Fundamental Rights
[259] The Convention on the Rights of the Child and the Convention on the Rights of Persons with Disabilities. See also the European Charter for Regional or Minority Languages (ETS No. 148)
[260] The International Convention on the Elimination of All Forms of Racial Discrimination, the Convention on the Elimination of All Forms of Discrimination against Women, and the Convention on Cybercrime and its Additional Protocol
[261] The Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (ETS No. 108), the EU General Data Protection Regulation (2016/679) and the EU Law Enforcement Directive (2016/680)
[262] Ibid, p. 19
[263] The Protocol will only enter into force when ratified, accepted or approved by all Parties to Treaty ETS 108, or on 11 October 2023 if there are 38 Parties to the Protocol at this date.
[264] E.g. in cybercrime. See the Convention on Cybercrime (ETS No. 185). As regards the EU, see e.g. the Cybersecurity Act (Regulation 2019/881) and the NIS Directive (2016/1148)

safeguards for the challenges presented by AI. However, more and more frameworks are being created within this (see the Commission's new proposal for an AI act later on).

AI and human rights

In a recent report by the European Economic and Social Committee on AI, reference is made to the broad societal impact of this technology.[265] This shows that AI has an impact on human rights, democracy and the rule of law.[266] What follows is a list of possible effects of AI on human rights. By taking an AI lifecycle approach to the analysis, the development, deployment and use phases of AI are taken into account. In a recent report by the CAHAI[267], two specific questions are raised that may be applicable to this deliverable with respect to human rights, namely:

- Impact of AI on Human Rights
- How to address the impact of AI on Human Rights

Impact of AI on Human Rights

CAHAI classifies four 'families of human rights' under the European Convention on Human Rights (ECHR), its Protocols European Social Charter (ESC) that are affected by AI:

- Respect for Human Dignity
- Freedom of the Individual
- Equality, Non-discrimination and Solidarity
- Social and Economic Rights

Several of these can be affected simultaneously, both negatively and positively.

Respect for Human Dignity

- Liberty and Security, Fair Trial, No Punishment without Law (art. 5, 6, 7 ECHR)

AI applications in law enforcement and the judiciary may increase biases or legal uncertainty because of its technology. For example, the AI may only be able to find correlations with other crimes or its specific technological background may remain a black box for judges and lawyers, making it difficult for them to understand its exact reasoning for a particular choice.

- Private and Family Life, Physical, Psychological and Moral Integrity (art. 8 ECHR)

AI can also have a major impact on privacy. CAHAI therefore also notes that impact on privacy goes beyond data privacy and indiscriminate processing of personal and non-personal data. Art. 8 ECHR is also applicable to (i) a person's (general) privacy, (ii) a person's physical, psychological or moral integrity and (iii) a person's identity and autonomy.

AI technology can then create a 'chilling effect' as in the case of mass surveillance applications such as facial recognition. People will then adjust their behaviour according to a certain norm in order to be less

[265] European Economic and Social Committee, Artificial Intelligence - The consequences of artificial intelligence on the (digital) single market, production, consumption, employment and society (own-initiative opinion), J C 288, 31.8.2017, p. 1–9
[266] Council of Europe, 'Towards Regulation of AI Systems - Global perspectives on the development of a legal framework on Artificial Intelligence (AI) systems based on the Council of Europe's standards on human rights, democracy and the rule of law', DGI (2020)16. Available; https://rm.coe.int/prems-107320-gbr-2018-compli-cahai-couv-texte-a4-bat-web/1680a0c17a, p. 21
[267] Ibid.; and see: Council of Europe, 'Feasibility Study', CAHAI(2020)23. Available: https://rm.coe.int/cahai-2020-23-final-eng-feasibility-study-/1680a0c6da

conspicuous. This shifts the power between the individual and the state or private organisations. The GDPR can offer a possible protection against the collection and processing of data, but this depends strongly on the exact type. Data not intended for identification may not be covered by the GDPR.

Freedom of the Individual

- Freedom of Expression and Information (art. 10 ECHR) en Freedom of Assembly and Association (art. 11 ECHR)

This right includes the freedom to have opinions and to receive information and ideas. AI can also have a chilling effect here in that people are less likely or more likely to voice their own opinions as AI technology provides less anonymity through its ability to track, identify, categorise or nudge people. In addition, AI technology can generate more personal information (or online context) and the ways in which this is done are not always transparent.

Equality, Non-discrimination and Solidarity

- Prohibition of Discrimination (art. 14 ECHR, Protocol 12)

As discussed earlier, AI can generate biases or magnify those of existing groups and reveal unrelated correlations. AI often works with large amounts of data and these systems can also reveal existing biases and marginalise the social control mechanisms that govern human behaviour. AI systems can only provide labels on found patterns and cannot understand the meaning of the input.

Biases in the system are often also the result of an accumulation of biased choices from the design of the technology itself. The developers themselves have certain biases that can be traced throughout the process, from the development of particular systems, to the input that is specifically fed into them or interpreted thereafter.

Social and Economic Rights

Finally, AI also has an effect on various rights in connection with social and economic rights because, for example, it "[…] increasingly being used to monitor and track workers, distribute work without human intervention and assess and predict worker potential and performance in hiring and firing situations".[268] As a consequence, Art 2, 3, 5 and 20 of the ESC can be violated. AO systems can affect working conditions so that the environment is no longer healthy for the employee (Art 2 and 3 ESC) or their right to organise is reduced by the self-awareness of constant monitoring (Art 5 ESC). Furthermore, AI systems can also contain biases when employment selections are made (art 20 ESC).

How to adress impact of AI on human rights

The impact of AI on human rights, among others, can be addressed by introducing "certain existing compliance, accountability and redress mechanisms could be further developed, and new mechanisms."[269] An important note is that AI systems are often difficult to fathom, so it is important that there is first a requirement for transparency about the use of AI systems. Among other things "an AI registry, which then specifies the risk class and required amount of transparency and accountability for a particular application". [270]

[268] Ibid., p. 28
[269] Ibid., p. 28 - 29
[270] Ibid., p. 32

The possibility of a legal requirement for an AI Human Rights (and Democracy and Rule of Law) Impact Assessment is therefore also being considered. This is currently being discussed and further developed by, amongst others, the CAHAI-PDG (Policy Development Group).[271] Currently, there are also other AI-specific impact assessments such as the Trustworthy AI Assessment List (designed by the High Level Expert Group on AI). A similar obligation for impact assessment already exists before the GDPR.[272]

5.3.3 Other international organisations

OECD

The OECD has adopted a (non-binding) *Recommendation on AI*[273] redefining its regulatory framework due to the rapidly changing socio-technical landscape in the last few decades.

Other countries outside of the European Union

With its *National Artificial Intelligence Initiative Act* of 2020[274], the United States of America (USA) has to date taken a rather hands-off approach towards AI regulation. This act is mainly focused on fostering investments and research and development in AI. In the meanwhile, the US Federal Trade Commission, trusts the existing USA legal framework to be sufficiently enough to address the risk of biases and discrimination associated with the growing use of AI systems at this stage. Moreover, as part of the newly established EU-US tech partnership (the Trade and Technology Council), the EU and the USA seek to develop a mutual understanding on the principles underlining trustworthy and responsible AI.[275] In September 2021, the United Kingdom (UK), published its National AI Strategy[276], enumerating in what way the UK will invest in AI applications and plans to present its AI regulation in 2022.

5.4 The EU framework

5.4.1 Current and applicable framework

Considering the fast development of AI systems and technologies in recent years, fundamental rights protected under the *EU Charter of Fundamental Rights*[277], as well as the safety risks for users when AI technologies are embedded in products and services, are raising concern. Especially in connection with the SOCIO-BEE project, AI systems may potentially violate fundamental rights such as the right to non-discrimination, freedom of expression, human dignity, personal data protection and privacy.[278]

Currently, the EU has no existing legal framework related to AI, but many initiatives and approaches have emerged over the years to accommodate these concerns, becoming a central policy question in the EU that are relevant for the coming years. Policy makers have been shown to prioritise the importance of a 'human-centred' approach to AI to ensure that Europeans can benefit from new technologies developed and functioning according to the EU values and principles.[279]

---

[271] Council of Europa, 'Human Rights, Democracy and Rule of Law Impact Assessment of AI systems', CAHAI-PDG(2021)02 Provisional
[272] Data Protection Impact Assessment (DPIA). See: Janssen, H.L. An approach for a fundamental rights impact assessment to automated decision-making, *International Data Privacy Law*, *10*(1), p. 76–106, doi:10.1093/idpl/ipz028
[273] OECD. 2019. Recommendation of the Council on Artificial Intelligence
[274] https://www.ai.gov/about/; https://www.congress.gov/116/crpt/hrpt617/CRPT-116hrpt617.pdf#page=1210
[275] https://digital-strategy.ec.europa.eu/en/policies/trade-and-technology-council; European Parliament, 'BRIEFING - Artificial intelligence act', PE 698.792 – November 2021
[276] https://www.gov.uk/government/publications/national-ai-strategy/national-ai-strategy-html-version
[277] Charter of Fundamental Rights of the European Union [2012/C] 326/02
[278] See for instance, High-Level Expert Group, Ethics Guidelines for Trustworthy AI, 2019.
[279] European Parliament, 'BRIEFING - Artificial intelligence act', PE 698.792 – November 2021, p. 2; Communication on Building Trust in Human-Centric Artificial Intelligence, COM(2019) 168,

Examples include the following:

- The Commissions' *White paper on Artificial Intelligence*[280]
  - This White Paper describes the European approach to AI.
- The European Parliament adopted three legislative resolutions on AI covering ethics, liability and intellectual property (IP)[281]

As described in a recent briefing of the European Parliament, the Commission initially adopted a soft-law approach[282] with its non-binding publications such as:

- Ethics Guidelines for Trustworthy AI[283]
  - These guidelines for trustworthy AI have been launched by the Commission in response to the EU AI Strategy.[284] Trustworthy AI consists of three components, which must be met throughout the system's life cycle:
    1. AI must be legal
    2. AI must be ethic
    3. AI must be robust
- Policy and investment recommendations[285]

Within the Ethics Guidelines for Trustworthy AI, the ethical elements are explicitly based on fundamental rights. The difference, however, is that these guidelines are not legally binding and therefore the Commission is working on a new proposal to regulate AI as set out in the White paper on AI. The EC once again points out that AI must be in line with the EU fundamental rights and that it also needs legislation to ensure these rights.[286]

In 2021 the Commission published its AI package, proposing new rules and actions to turn Europe into a global hub for trustworthy AI. The packages consisted of a Communication on Fostering a European approach to Artificial Intelligence[287], thereby shifting towards a legislative approach because it called for the adoption of a new regulatory framework on AI. It also contains a revised coordinated plan on AI which

[280] European Commission – WHITE PAPER On Artificial Intelligence – A European approach to excellence and trust, COM/2020/65 final

[281] European Parliament, Legislative train schedule – A Europe fit for the digital Age, https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-white-paper-artificial-intelligence-and-follow-up

[282] "The term soft law is used to denote agreements, principles and declarations that are not legally binding. Soft law instruments are predominantly found in the international sphere. UN General Assembly resolutions are an example of soft law. Hard law refers generally to legal obligations that are binding on the parties involved and which can be legally enforced before a court." ECCHR, (n.d.), https://www.ecchr.eu/en/glossary/hard-law-soft-law/

[283] European Commission, High-level expert group on Artificial Intelligence, Ethics Guidelines for a Trustworthy AI, 2019, https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

[284] European Commission, 'Communication from the commission – Artificial Intelligence for Europe', COM(2018) 237 final

[285] European Commission, High-Level Expert Group on AI (AI HLEG), 2019, https://digital-strategy.ec.europa.eu/en/library/policy-and-investment-recommendations-trustworthy-artificial-intelligence

[286] Council of Europe, 'Towards Regulation of AI Systems - Global perspectives on the development of a legal framework on Artificial Intelligence (AI) systems based on the Council of Europe's standards on human rights, democracy and the rule of law', DGI (2020)16. Available; https://rm.coe.int/prems-107320-gbr-2018-compli-cahai-couv-texte-a4-bat-web/1680a0c17a

[287] European Commission, Communication on Fostering a European Approach to Artificial Intelligence, 2021, https://digital-strategy.ec.europa.eu/en/library/communication-fostering-european-approach-artificial-intelligence

builds on the previous coordinated plan of 2018, focusing on the strong collaboration between the Commission and the Member States.[288]

"Excellence and trust are at the heart of the EU's approach to artificial intelligence, seeking to boost research and industrial capacity and to safeguard fundamental rights."[289]

5.4.1.1 Safety requirements

The partners follow closely all the relevant developments and in particular, the work of the European Union Cybersecurity Agency (ENISA). Specifically, the technical partners will take into consideration guidelines and recommendations included among others in: ENISA, Securing Machine Learning Algorithms (December 2021).[290]

5.4.2 Future developments to keep an eye on

5.4.2.1 Proposal for AI Regulation

On April 21, 2021, the European Commission adopted a proposal for a regulation on AI systems, *The Artificial Intelligence Act*[291], which would be the first legal framework on AI to harmonize rules regarding AI use in the EU and be applicable to all AI systems placed on the market or used in the European Union. This new set of rules would complement and be designed following the logic of the existing EU rules on safety products. The adoption of the rules from the AI act would be parallel to the new *Machinery Regulation*[292] which will adapt existing safety rules to a new generation products.

With the new proposal, the Commission has taken a technology-neutral definition of AI systems in EU law in which the AI act also proposes a classification for AI systems with different requirements and obligations tailored on a 'risk-based approach'. "On the other hand, the AI Regulation includes a number of provisions intended to promote the development and uptake of AI systems in the European Union (EU). The AI Regulation also creates a new regulatory framework, with a European Artificial Intelligence Board overseeing and co-ordinating enforcement. The AI Regulation envisages a two-year period for application following adoption and publication of the final regulation, meaning that the new requirements could apply as early as 2024".[293]

A brief overview

Definition

> *"'Artificial intelligence system' (AI system) means software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined*

[288] European Commission, A European approach to artificial Intelligence, https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence
[289] Ibid.
[290] ENISA, Securing Machine Learning Algorithms, 2021, [Online]. Available: https://www.enisa.europa.eu/publications/securing-machine-learning-algorithms
[291] European Commission, 'Proposal for a regulation of the European Parliament and of the council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain Union legislative acts' COM(2021) 206 final
[292] European Commission, 'Proposal for a Regulation of the European Parliament and of the Council on machinery products', COM(2021) 202 final
[293] Modrall, J. (2021, April). *EU proposes new Artificial Intelligence Regulation*. Norton Rose Fulbright. https://www.nortonrosefulbright.com/en-gb/knowledge/publications/fdfc4c27/eu-to-propose-new-artificial-intelligence-regulation

objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with".[294]

It is important to note that the legal definition of 'AI systems' given in the new proposed AI act has been heavily debated and criticized.[295] The definition would lack clarity and may also lead to legal uncertainty. This could be especially the case with systems that would not qualify as AI systems under the draft text, while their use may have an adverse impact on fundamental rights.[296]

Classification

This classification of AI systems is divided into four categories and should ensure that AI systems are safe, transparent, ethical and free of prejudice, and are therefore controlled by humans. The four categories are:

- Unacceptable risk: Prohibited AI practices
  - Title II (Article 5) of the proposed AI act explicitly bans harmful AI practices that are considered to be a clear threat to people's safety, livelihoods and rights, because of the 'unacceptable risk' they create. Accordingly, it would be prohibited to place on the market, put into services or use in the EU.[297]
- High-risk: Regulated high-risk AI systems
  - Title III (Article 6) of the proposed AI act regulates 'high-risk' AI systems that create adverse impact on people's safety or their fundamental rights. The draft text distinguishes between two categories of high-risk AI systems.[298]
    - High-risk AI systems used as a safety component of a productor as a product falling under Union health and safety harmonisation legislation(e.g. toys, aviation, cars, medical devices, lifts).
    - High-risk AI systems deployed in eight specific areas identified in Annex III, which the Commission would be empowered to update as necessary by way of a delegated act (Article 7)
- Limited risk: Some AI systems will be subject to a limited set of obligations (e.g. transparency obligations)
  - The AI systems presenting 'limited risk', such as systems that interacts with humans (i.e. chatbots), emotion recognition systems, biometric categorisation systems, and AI systems that generate or manipulate image, audio or video content (i.e. deepfakes), would be subject to a limited set of transparency obligations (Title IV).[299]
- Low or minimal risk: No obligations

[294] Ibid., art 3(1)
[295] IPlens, A PROPOSAL FOR (AI) CHANGE? A succinct overview of the Proposal for Regulation laying down harmonised rules on Artificial Intelligence, 11 may 2021, *https://iplens.org/category/artificial-intelligence/*
[296] Smuha, N., and others, *How the EU Can Achieve Legally Trustworthy AI: A Response to the European Commission's Proposal for an Artificial Intelligence Act*, Elsevier, August 2021. There are also calls for a shift in approach, to identify problematic practices that raise questions in terms of fundamental rights, rather than focusing on definitions; Veale M., Zuiderveen Borgesius F., *Demystifying the draft EU AI Act*, 22(4) *Computer Law Review International*, July 2021.
[297] European Parliament, 'BRIEFING - Artificial intelligence act', PE 698.792 – November 2021, p. 5
[298] Ibid., p. 5-6
[299] Ibid., p. 6

- All other AI systems presenting only low or minimal risk could be developed and used in the EU without conforming to any additional legal obligations. However, the proposed AI act envisages the creation of codes of conduct to encourage providers of non-high-risk AI systems to voluntarily apply the mandatory requirements for high-risk AI systems (Title IX).[300]

Connection to other developments

Currently, there are also other European initiatives in the digital sector that are also relevant to the AI act because they share related provisions. These are, among others the Data Governance Act, Digital Services Act, Digital Markets Act, Data Act and the reform of EU antitrust policy.

On 22 January 2022, the "Declaration of Digital Principles" was also adopted by the EC. “This initiative proposes a set of principles that should define the ‘European way’ for the digital society. The goal is to inform people and provide a reference for policymakers and digital operators in their actions in the digital environment”.[301]

The EU aims for a 'human-centred digital transformation'. This means that technology works for people and respects the values and norms of all of us online as well as offline. Specific for AI include chapter three of the Declaration that contains commitments to 'freedom of choice'. The EU wants people to be able to make their own informed choices online. To ensure this, it is trying to help EU citizens do so through various commitments. It also wants to protect citizens against possible risks.. “This includes being transparent about the use of algorithms and artificial intelligence, a new obligation to be set under our Digital Services and Artificial Intelligence Acts”.[302]

5.5 Specific considerations: children and elderly persons

5.5.1 Children and new (AI) technologies

Modern information and communication technologies play an increasingly important role in children's lives. Measures are therefore needed to ensure equal and safe access. Since 2016, the CoE has been working on the 'rights of the child in the digital environment', to be promoted by its ‘Strategy for the Rights of the Child (2016-2021)’.[303] To do this successfully, the CoE utilizes a key instrument namely:

- ‘Guidelines to respect, protect and fulfil the rights of the child in the digital environment’ adopted by the Committee of Ministers as CM/Rec(2018)7 in 2018[304]
  - These guidelines “balance the protection of children in the digital world with the promotion of their positive rights as end users of digital technologies in their own right”.[305]

[300] Ibid. p. 7
[301] See: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13017-Declaration-of-Digital-Principles-the-%E2%80%98European-way%E2%80%99-for-the-digital-society_en
[302] See: https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_22_625
[303] CoE, ‘Handbook for policy makers on the rights of the child in the digital environment’, Available: https://rm.coe.int/publication-it-handbook-for-policy-makers-final-eng/1680a069f8, p. 5
[304] CoE, ‘Guidelines to respect, protect and fulfil the rights of the child in the digital environment’, Available: https://rm.coe.int/guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-th/16808d881a
[305] Ibid., p. 5

Subsequently, the CoE has also recently published a 'Handbook for policy makers on the rights of the child in the digital environment' that serves to establish a common approach among all stakeholders, either through national legislation, developing strategic partnerships etc. In this manual, there are some tables that address the 'opportunities and risks related to AI in the context of children's rights in the digital environment'. For this deliverable, they are then taken from this manual and shown on the following pages.[306]

[306] Ibid., p. 78-80

TYPE OF MEASURE	SPECIFIC PRINCIPLE/RIGHT	OPPORTUNITIES RELATED TO AI (EXAMPLES)	RISKS RELATED TO AI (EXAMPLES)
Operational principles and measures	Participation, right to engage in play and right to assembly and association	▸ AI in interactive toys and other cevices can personalise and enhance children's play experience, assist in develooment of social skills, non-formal education (e.g. "coding toys") or development of healthy habits	▸ AI toys and other devices can store various types of children's data: data protection and security (hacking) risks, ethical questions of whether businesses have a duty to report and share collected data which raises issues about a child's safety ▸ AI toys and other devices connected to the internet: risk of being hacked and "controlled" by an external actor ▸ AI toys and other devices may enable location detection and tracking, surveillance of the child, by parents/caregivers and business enterprises: risk of breach of privacy and data protection ▸ AI devices which enable commands/orders: possible negative effect on children's development, behaviours and attitudes, particularly if devices have predominantly "female" characters
	Privacy and data protection	▸ Privacy automation (i.e. automatic enforcement of data privacy through computer systems) may contribute to or even enhance protection of privacy and data online	▸ AI devices collect and store children's data, risk to privacy and data protection rights if processing activities do not comply with data protection laws ▸ Collection and analysis of "big data", including online and in educational and medical fields: risk to children's data protection and privacy rights, right to non-discrimination, right to development ▸ Use of AI to profile children through automated processing of personal data for purposes which might negatively affect children (including commercial exploitation): risk to data protection rights and further protection issues (see "protection and safety")

Figure 6. Opportunities and risks related to AI in the context of children's rights in the digital environment (1)

TYPE OF MEASURE	SPECIFIC PRINCIPLE/RIGHT	OPPORTUNITIES RELATED TO AI (EXAMPLES)	RISKS RELATED TO AI (EXAMPLES)
Operational principles and measures	Participation, right to engage in play and right to assembly and association	▸ AI in interactive toys and other devices can personalise and enhance children's play experience, assist in development of social skills, non-formal education (e.g. "coding toys") or development of healthy habits	▸ AI toys and other devices can store various types of children's data: data protection and security (hacking) risks, ethical questions of whether businesses have a duty to report and share collected data which raises issues about a child's safety ▸ AI toys and other devices connected to the internet: risk of being hacked and "controlled" by an external actor ▸ AI toys and other devices may enable location detection and tracking, surveillance of the child, by parents/caregivers and business enterprises: risk of breach of privacy and data protection ▸ AI devices which enable commands/orders: possible negative effect on children's development, behaviours and attitudes, particularly if devices have predominantly "female" characters
	Privacy and data protection	▸ Privacy automation (i.e. automatic enforcement of data privacy through computer systems) may contribute to or even enhance protection of privacy and data online	▸ AI devices collect and store children's data, risk to privacy and data protection rights if processing activities do not comply with data protection laws ▸ Collection and analysis of "big data", including online and in educational and medical fields: risk to children's data protection and privacy rights, right to non-discrimination, right to development ▸ Use of AI to profile children through automated processing of personal data for purposes which might negatively affect children (including commercial exploitation): risk to data protection rights and further protection issues (see "protection and safety")

Figure 7. Opportunities and risks related to AI in the context of children's rights in the digital environment (2)

TYPE OF MEASURE	SPECIFIC PRINCIPLE/RIGHT	OPPORTUNITIES RELATED TO AI (EXAMPLES)	RISKS RELATED TO AI (EXAMPLES)
Operational principles and measures	Right to education	▶ Adaptive learning systems tailored to children's needs and maturity ▶ Assisting early intervention programmes: AI precicts student outcomes and identifies those at risk of dropping out of school systems ▶ Enhanced learning experience: investment in AI in classrooms ▶ Increased teacher capacity: use of AI in teacher training and teaching methods ▶ AI in digital literacy initiatives/programmes ensure children are empowered and supported to safely use AI	▶ Classroom behaviour and performance monitoring: risk of breach of children's privacy and chilling effect on their ability to freely act and express themselves ▶ Collection of personal data through AI-powered educational tools: risk of data protection violations/breaches ▶ Conveying stereotyped or prejudiced information: risk of replicating/worsening inequalities ▶ Poor/lacking AI literacy and education leaves children exposed to risks and unable to take full advantage of AI
	Right to protection and safety	▶ Filtering systems can block access to abusive or illegal content ▶ AI can be used to assist identification, analysis, removal and reporting of child sexual abuse material and other forms of online sexual exploitation and abuse, as well as identification of child victims and abusers: greater potential speed and efficiency, lower exposure and emotional toll on relevant professionals	▶ Manipulation of algorithms to promote disguised/targeted forms of commercial content/advertising, or child profiling used to enable "micro-targeting" of commercial advertising ▶ Use of AI to produce highly attractive and potentially "addictive" games, apps, toys etc.: risk of over-use and development of unhealthy habits ▶ AI technologies used to carry out child sexual exploitation and abuse, including, grooming (e.g. convincing fake online profiles), production of highly realistic child sexual abuse material, which can also circumvent hash systems, simulation of scenarios of abuse (e.g. interactive "games", dolls/robots) ▶ Risk of increased difficulty in identifying victims, e.g. where "deepfake" technology is used to synthesise pre-existing images
	Remedies	▶ AI technologies may assist in collection of complaints (messaging or chatbots), complaint analysis and decision-making: potentially more efficient decision-making and quicker provision of remedies	▶ Risk of lack of complaints mechanisms/systems of redress in relation to AI services, technologies, etc. ▶ Where AI is used in complaints mechanisms: risks of unethical system design, error, opaque decision-making algorithms and criteria, affecting legitimacy and/or ability to challenge decisions

Figure 8. Opportunities and risks related to AI in the context of children's rights in the digital environment (3)

5.6 Preliminary recommendations

Seven principles

The Ethics Guidelines for Trustworthy Artificial Intelligence (AI) published by the High-Level Expert Group on Artificial Intelligence contains seven key requirements that must be met for the application and realisation of trustworthy Artificial Intelligence (AI). "These requirements apply to various stakeholders who are part of the life cycle of KI systems: developers, installers and end-users, as well as society at large.".[307] Depending on the stakeholders, there are different roles to play in ensuring that the requirements are met:

- Developers must implement the requirements and apply them to the design and development processes
- Installers must ensure that the systems they use and the products and services they offer meet the requirements
- End-users and society at large must be made aware of these requirements and have the opportunity to request that they are met

The list of requirements below is non-exhaustive (and non-hierarchical) and includes systemic, individual and societal aspects:

1) Human agency and oversight
2) Technical robustness and safety
3) Privacy and data governance
4) Transparency
5) Diversity, non-discrimination and fairness
6) Environmental and societal well-being
7) Accountability

AI Impact Assessment

The partners in Socio Bee take the AI Impact Assessment (AIIA) into account. This AIIA is not mandatory, but should be seen as a support for the use of AI. Companies and organisations remain responsible for the choices they make in relation to AI, but with this AIIA, risks and costs can be reduced. It is a guide that can help partners find the right framework of standards (legal and ethical) and determine the relevant trade-offs.

In Annex 1 - Artificial Intelligence Code of Conduct of the 'Artificial Intelligence Impact Assessment' of the ECP[308], the basis for the AIIA can be found.

It consists of two parts, namely

- Ethical principles

[307] See: European Commission, High-level expert group on Artificial Intelligence, Ethics Guidelines for a Trustworthy AI, 2019, https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai, p. 17

[308] See: https://static1.squarespace.com/static/5b7877457c9327fa97fef427/t/5c368c611ae6cf01ea0fba53/1547078768062/Artificial+Intelligence+Impact+Assessment+-+English.pdf

- Rules of practice

In Annex 2 – AIIA roadmap it shows the different steps and questions that can be used to check whether an AIIA should be made in the first place.

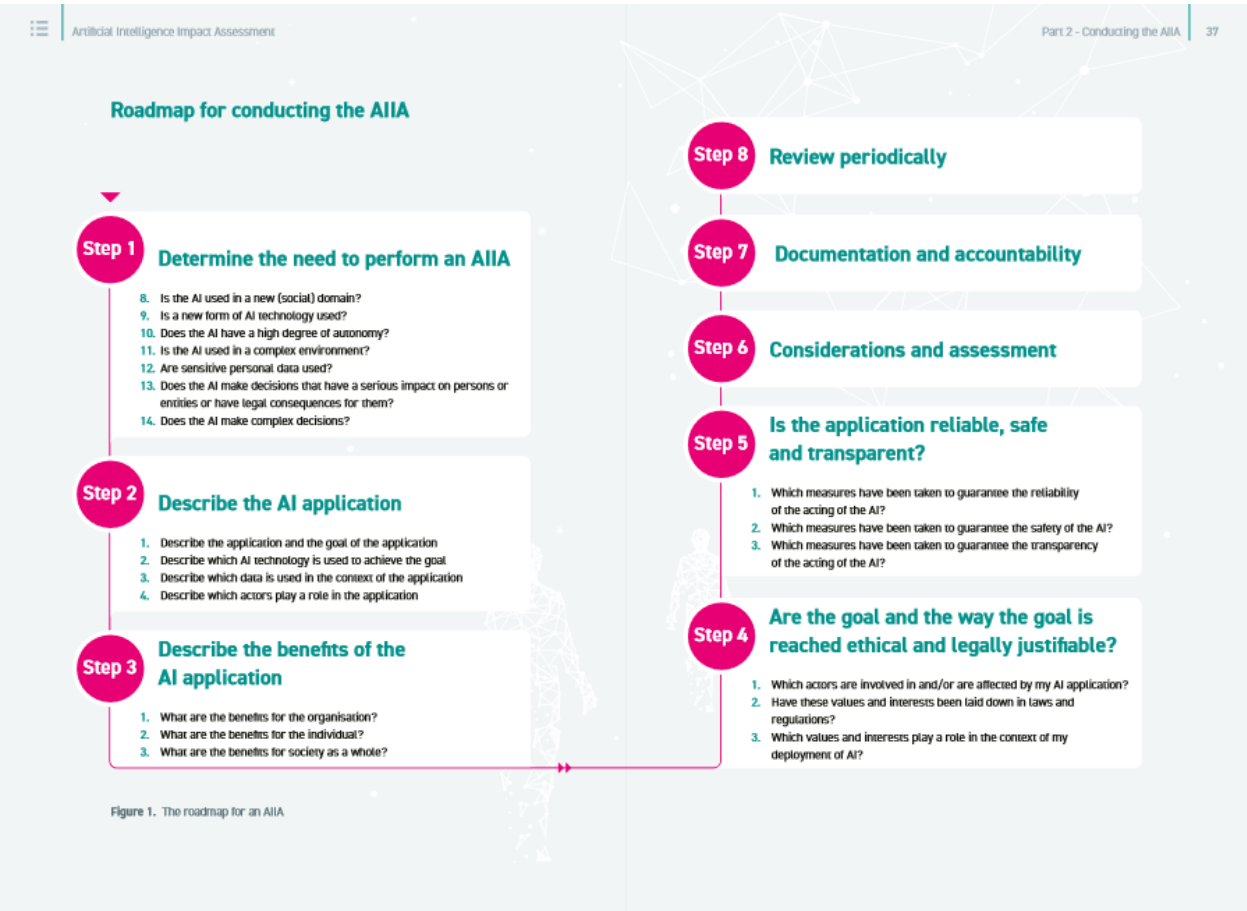

Figure 9. Roadmap for conducting the AIIA[309]

Following the debate

The Socio Bee partners will closely monitor the debates on the AI Act. These can also be followed through the legislative train schedule of the EP among others.[310] It is also important that the impact of developments on the elderly and children is always taken into account.

6 Conclusions

This deliverable provided an initial examination of the legal and regulatory requirements relevant to the Socio Bee project. It discussed in broad terms the relevant frameworks that should be taken into considerations throughout the project. The first part began by explaining the relevant developments, state of the art and future challenges of citizen science in relation to air pollution. Secondly, the

[309] Platform for the Information Society, 'Artificial Intelligence Impact Assessment', Available at: https://ecp.nl/wp-content/uploads/2019/01/Artificial-Intelligence-Impact-Assessment-English.pdf, p. 19
[310] See : https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-data-act

deliverable described the use of drones in the European Union. Due to recent legal developments in the EU regarding drones, there is currently a transition period in the Member States. Next, the use of wearables was discussed. Since wearables are part of the Internet of Things, it was necessary to consider both components. Finally, the role of Artificial Intelligence and Machine Learning in the project was also considered. Both technologies will have a major impact in the future, which is why there are currently many debates and initiatives being drawn up by the European Union.

As for the legal and regulatory frameworks discussed, VUB-LSTS will keep an eye on further developments throughout the project. This will be necessary as, firstly, there are many new initiatives on the agenda of the European Union and, secondly, the technologies used are evolving rapidly.

D3.1 will provide input to D1.5 (Data Management Plan) and D6.1 (Impact Assessment Model). In those two next deliverables (and respective WPs), topics covered here will be further explored and detailed, in cooperation with the consortium. In D1.5, from a research data management and ethics requirements point of view. In D6.1, with respect to the preparation of a holistic impact assessment method.

7 References

Literature

Arnstein, S.R. (1969). "A Ladder of Citizen Participation. *Journal of the American Planning Association, 35*(4), 216-224. doi:10.1080/01944366908977225

Bauer, D., Wutzke, R., & Bauernhansl, T. (2016). Wear@Work – A New Approach for Data Acquisition Using Wearables. *Procedia CIRP*. 50. 529-534. doi:10.1016/j.procir.2016.04.121.

Berti Suman, A., & Pierce, R. (2018). Challenges for citizen science and the EU open science agenda under the GDPR. *European Data Protection Law Review,* 4(3), 284-295. doi10.21552/edpl/2018/3/7

Berti Suman, A., & van Geenhuizen, M. (2020) Not just noise monitoring: rethinking citizen sensing for risk-related problem-solving, *Journal of Environmental Planning and Management*, *63*(3), 546-567, doi:10.1080/09640568.2019.1598852
Cavoukian, A. (2012). Privacy and Drones: Unmanned Aerial Vehicles. Information and Privacy Commissioner, Ontario

Chilvers, J., & Kearnes, M. (2020). Remaking Participation in Science and Democracy. *Science, Technology, & Human Values*, *45*(3), p. 347–380. doi:10.1177/0162243919850885

De Marchi, B., Funtowicz, S., & Guimarães-Pereira, A. (2001). From the right to be informed to the right to participate: Responding to the evolution of European legislation with ICT. *International Journal of Environment and Pollution*, 15(1), 1–21.

Eleonora, B. (2020). From here to 2023: Civil drones operations and the setting of new legal rules for the european single sky. *Journal of Intelligent & Robotic Systems,* 100(2), 493-503. doi:10.1007/s10846-020-01185-1, p. 499

Bauer et al, 2016; p. 531; Huang P. Promoting Wearable Computing. In: Jin Q, Li J, Zhang N, Cheng J, Yu C, Noguchi S, editors. *Enabling Society with Information Technology*. Tokyo: Springer Japan; 2002. p. 367-76 .

Finn, R.L., Wright, D. (2016). Privacy, data protection and ethics for civil drone practice: a survey of industry, regulators and civil society organisations. *Comp. Law & Sec. Rev.* 32, 577–586

Finn, R. (n.d.) 'Privacy and Data Security for IoT – what are the risks in monitoring our environment?'. [Online]. Available: https://www.trilateralresearch.com/privacy-and-data-security-for-iot-what-are-the-risks-in-monitoring-our-environment/; On General Data Protection Regulation Vulnerabilities and Privacy Issues, for Wearable Devices and Fitness Tracking Applications

Gijsel, L., Huye, T., & Van Hoyweghen, I. (2019). *Citizen science: hoe burgers de wetenschap uitdagen*. Kalmthout: Pelckmans Pro. [Dutch]

Haklay, M. (2013). Chapter 7 - Citizen Science and Volunteered Geographic Information: Overview and Typology of Participation. In D. Sui, S., Elwood, & M., Goodchild (Reds.). *Crowdsourcing Geographic Knowledge: Volunteered Geographic Information (VGI) in Theory and Practice* (pp. 105-122). New York: Springer.

Heigl, F., Kieslinger, B., Paul, K.T., Uhlik, J., & Dörler, D. (2019). Toward an international definition of citizen science. *PNAS, 116*(17), 8089-8092. doi:10.1073/pnas.1903393116

Irwin, A. (1995*). Citizen Science: A Study of People, Expertise, and Sustainable Development. Environment and Society.* London: Routledge.

Janssen, H.L. An approach for a fundamental rights impact assessment to automated decision-making, *International Data Privacy Law*, *10*(1), p. 76–106, doi:10.1093/idpl/ipz028

King, A. C., King, D. K., Banchoff, A., Solomonov, S., Ben Natan, O., Hua, J., Gardiner, P., Rosas, L. G., Espinosa, P. R., Winter, S. J., Sheats, J., Salvo, D., Aguilar-Farias, N., Stathi, A., Akira Hino, A., Porter, M. M., & Our Voice Global Citizen Science Research Network, O. (2020). Employing Participatory Citizen Science Methods to Promote Age-Friendly Environments Worldwide. *International journal of environmental research and public health*, *17*(5), 1541. doi.org:10.3390/ijerph17051541

Maniadaki, M., Papathanasopoulos, A., Mitrou, L., & Efpraxia-Aithra Maria. (2021). Reconciling remote sensing technologies with personal data and privacy protection in the european union: Recent developments in greek legislation and application perspectives in environmental law. *Laws*, 10(2), 33. doi:10.3390/laws10020033

Makuch, K.E., & Aczel, M.R. (2018). Children and citizen science. In: Hecker, S., Haklay, M., Bowser, A., Makuch, Z., Vogel, J. & Bonn, A. 2018. *Citizen Science: Innovation in Open Science, Society and Policy*. UCL Press, London. doi:10.14324 /111.9781787352339

Mateusz, G. (2018). Analysis of international law on Unmanned Aerial Vehicles through the prism of European Union law, *Przegląd Europejski*, *2018*(4). Doi:10.5604/01.3001.0013.3455, p. 76; See also: ICAO (2015), Manual on Remotely Piloted Aircraft Systems (RPAS), First Edition, Quebec.,

Piwek, L., Ellis, D. A., Andrews, S. and Joinson, A. (2016), The rise of consumer health wearables: Promises and barriers*, PLoS Med*, Vol. 13, No. 2, pp. e1001953, available at https://doi.org/10.1371/journal.pmed.1001953.

Strasser, B. J., Baudry, J., Mahr, D., Sanchez, G. and Tancoigne, E. (2019) 'Citizen Science'? Rethinking Science and Public Participation, *Science & Technology Studies*, *32*(2), p. 52–76. doi:10.23987/sts.60425

Schade et al. (2021). Chapter 18 – Citizen Science and Policy. In K., Vohland, A., L.and-Zandstra., L., Ceccaroni, R., Lemmens, J., Perelló, M., Ponti, R., Samson, & K., Wagenknecht (Eds.). *The Science of Citizen Science.* (pp. 357) New York: Springer.

Smuha N., and others, *How the EU Can Achieve Legally Trustworthy AI: A Response to the European Commission's Proposal for an Artificial Intelligence Act,* Elsevier, August 2021.

Suman, A. B. (2021). Citizen Sensing from a Legal Standpoint: Legitimizing the Practice under the Aarhus Framework, *Journal for European Environmental & Planning Law*, *18*(1), 8-38. doi: https://doi.org/10.1163/18760104-18010003

van der Veer, L. (2020). *Op weg naar een democratisering van wetenschappelijk onderzoek? Een studie naar de verschillende gedaantes van Citizen Science in Vlaanderen* (Master's thesis, KU Leuven, Leuven, Belgium). [Dutch]

Wei, Jh. 'How wearables intersect with the cloud and the Internet of Things: Considerations for the developers of wearables', *IEEE Consumer Electronics Magazine*, Vol. 3, No. 3, pp. 53–56

Zakaria, N.A.; Abidin, Z.Z.; Harum, N.; Hau, L.C.; Ali, N.S.; Jafar, F.A. Wireless Internet of Things-Based Air Quality Device for Smart Pollution Monitoring. *Int. J. Adv. Comput. Sci. Appl*. 2018

Case law

Court of Justice of the European Union

CJEU, Case C-59/89 Commission v Germany
CJEU, Case C-404/13 ClientEarth
CJEU, Google LLC v Bundesrepublik Deutschland (Fourth Chamber) of 13 june 2019, Case C-193/18

Documents of European Organisations

European Commission

ALADDIN [Project 740859], D3.1 – Data protection, Social, Ethical and Legal Frameworks, p. 31; Regulation (EC) 216/2008

H2020-LC-GD-2020: SOCIO-BEE, GA No: 101037648

Communication from the Commission to the European Parliament, the European Council , the Council , the European Economic and Social Committee and the Committee of the Regions on Artificial Intelligence for Europe, Brussels ,25.4.2018 COM(2018) 237 final

Communication on Building Trust in Human-Centric Artificial Intelligence, COM(2019) 168

European Commission, 'How a European Cyber Resilience Act will help protect Europe', [Blog Post], Available at: https://ec.europa.eu/commission/commissioners/2019-2024/breton/blog/how-european-cyber-resilience-act-will-help-protect-europe_en

European Commission, COMMISSION STAFF WORKING DOCUMENT, Best Practices in Citizen Science for Environmental Monitoring, SWD(2020) 149 final

European Commission, Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee, the Committee of the Regions and the European Investment Bank - A clean planet for all: A long-term European strategic vision for a prosperous, modern, competitive and climate-neutral economy [COM(2018)773 final]. Brussels, 28.11.2018

European Commission, 'COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL EMPTY - Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union', COM(2019) 250 final

European Commission, 'Communication from the commission – Artificial Intelligence for Europe', COM(2018) 237 final

European Commission, 'Horizon 2020 – Work Programme 2018-2020, Information and Communication Technologies', Avaible: https://ec.europa.eu/research/participants/data/ref/h2020/wp/2018-2020/main/h2020-wp1820-leit-ict_en.pdf

European Commission, 'Smart Wearables Reflection and Orientation Paper', December 2017

European Commission, 'Smart Wearables Reflection and Orientation Paper – Including Feedback from Stakeholders, https://digital-strategy.ec.europa.eu/en/news/feedback-stakeholders-smart-wearables-reflection-and-orientation-paper

European Commission, 'Union of Equality - Strategy for the Rights of Persons with Disabilities 2021-2030', Brussels , 3.3.2021 COM(2021) 101 final

European Commission – WHITE PAPER On Artificial Intelligence – A European approach to excellence and trust, COM/2020/65 final

M/536 COMMISSION IMPLEMENTING DECISION C(2015) 5376 final of 4.8.2015 on a standardisation request to the European Committee for Electrotechnical Standardisation and to the European Telecommunications Standards Institute as regards radio equipment in support of Directive 2014/53/EU of the European Parliament and of the Council

Other EU organisations

European Environment Agency, 'Air Quality in Europe – 2020 Report', 9. https://www.eea.europa.eu/publications/air-quality-in-europe-2020-report

EEA Report No 19/2019 Assessing air quality through citizen science: https://www.eea.europa.eu/publications/assessing-air-quality-through-citizen-science

EASA's Easy Access Rules for Unmanned Aircraft Systems. https://www.easa.europa.eu/document-library/easy-access-rules/easy-access-rules-unmanned-aircraft-systems-regulation-eu
EASA, 'Drones (UAS) FAQ', [Online]. Available: https://www.easa.europa.eu/the-agency/faqs/drones-uas; Regulation (EU) 2019/947

ENISA, Good Practices for Security of IoT - Secure Software Development Lifecycle, 2019, [Online]. Available: https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot-1

ENISA, Guidelines for Securing the Internet of Things, 2020, [Online]. Available: https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things

ENISA, 'Towards a Framework for Policy Development in Cybersecurity -Security and Privacy Considerations in Autonomous Agents'. 2018, [Online]. Available: https://www.enisa.europa.eu/publications/considerationsin-autonomous-agents.

ENISA, Securing Machine Learning Algorithms, 2021, [Online]. Available: https://www.enisa.europa.eu/publications/securing-machine-learning-algorithms

European Data Protection Board, 'Guidelines 4/2019 on Article 25 Data Protection by Design and by Default'. 2019, [Online]. Available:https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201904_dataprotection_by_design_and_by_defa ult.pdf.

Eurofound, WORKING PAPER, Wearable devices: Implications of game-changing technologies in services in Europe, p. 7

Eurofound, 'Wearable devices: Implications of game-changing technologies in services in Europe'

European Economic and Social Committee, Artificial Intelligence - The consequences of artificial intelligence on the (digital) single market, production, consumption, employment and society (own-initiative opinion), J C 288, 31.8.2017

European Parliament, 'BRIEFING - Artificial intelligence act', PE 698.792 – November 2021

European Parliament, 'Review of the Directive of Network and Information Systems', Available at: https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-review-of-the-nis-directive

SESARJU, "U-Space Blueprint" (June 9, 2017). See: https://www.sesarju.eu/u-space-blueprint.91

Documents of International Organisations

United nations

Report of the Special Rapporteur on human rights and the environment to the UN General Assembly, *Right to breathe clean air*, A/HRC/40/55, 8 January 2019. https://undocs.org/A/HRC/40/55

UN Special rapporteur on human rights and the environment, *Recognition of the Right to a Healthy Environment in Constitutions, Legislation and Treaties*, (Annual thematic report, 30 December 2019), A/HRC/43/53

The Sustainable Development Goals. [Online]. Available: https://sdgs.un.org/goals

UNEP. Environmental Assembly. Available at: http://web.unep.org/environmentassembly/major-groups-and-stakeholder-science-and-technology

ICAO (2011), Unmanned Aircraft Systems (UAS), Cir.328.AN/190, Montreal

Council of Europe

Council of Europe, 'Feasibility Study', CAHAI(2020)23. Available: https://rm.coe.int/cahai-2020-23-final-eng-feasibility-study-/1680a0c6da, p. 18

Council of Europe, 'Human Rights, Democracy and Rule of Law Impact Assessment of AI systems', CAHAI-PDG(2021)02 Provisional

Council of Europe, 'Handbook for policy makers on the rights of the child in the digital environment', Available: https://rm.coe.int/publication-it-handbook-for-policy-makers-final-eng/1680a069f8

Council of Europe, 'Towards Regulation of AI Systems - Global perspectives on the development of a legal framework on Artificial Intelligence (AI) systems based on the Council of Europe's standards on human rights, democracy and the rule of law', DGI (2020)16. Available; https://rm.coe.int/prems-107320-gbr-2018-compli-cahai-couv-texte-a4-bat-web/1680a0c17a

European legislation

Council of Europe

European Union

Commission Delegated Regulation (EU) 2019/945 of 12 March 2019 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems, OJ L 152, 11.6.2019

Commission Delegated Regulation (EU) 2022/30 of 29 October 2021 supplementing Directive 2014/53/EU of the European Parliament and of the Council with regard to the application of the essential requirements referred to in Article 3(3), points (d), (e) and (f), of that Directive (Text with EEA relevance), OJ L 7, 12.1.2022

Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on the rules and procedures for the operation of unmanned aircraft, OJ L 152, 11.6.2019, p. 45–71

Commission Implementing Regulation (EU) 2021/664 of 22 April 2021 on a regulatory framework for the U-space (Text with EEA relevance), C/2021/2671; OJ L 139, 23.4.2021, p. 161-183

Cover Regulation to implementing Regulation (EU) 2019/947

Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety, OJ L 11 p. 4–17'. Jan. 15, 2002

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002, p. 37–47

Directive 2004/107/EC of the European Parliament and of the Council of 15 December 2004 relating to arsenic, cadmium, mercury, nickel and polycyclic aromatic hydrocarbons in ambient air, OJ L 23, 26.1.2005, p. 3–16

Directive 2008/50/EC of the European Parliament and of the Council of 21 May 2008 on ambient air quality and cleaner air for Europe, OJ L 152, 11.6.2008, p.1-44

Directive 2009/48/EC of the European Parliament and of the Council of 18 June 2009 on the safety of toys (OJ L 170, 30.6.2009, p. 1)

Directive 2009/33/EC of the European Parliament and of the Council of 23 April 2009 on the promotion of clean and energy-efficient road transport vehicles (Text with EEA relevance), OJ L 120, 15.5.2009, p. 5–12

DECISION No 1386/2013/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 20 November 2013 on a General Union Environment Action Programme to 2020 'Living well, within the limits of our planet' (Text with EEA relevance). L 352/171

Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC Text with EEA relevance, OJ L 153, 22.5.2014

Directive (EU) 2015/2193 of the European Parliament and of the Council of 25 November 2015 on the limitation of emissions of certain pollutants into the air from medium combustion plants (Text with EEA relevance), OJ L 313, 28.11.2015, p. 1–19

Directive (EU) 2016/2284 of the European Parliament and of the Council of 14 December 2016 on the reduction of national emissions of certain atmospheric pollutants, amending Directive 2003/35/EC and repealing Directive 2001/81/EC (Text with EEA relevance), OJ L 344, 17.12.2016, p. 1–31

Directive (EU) 2019/882 of the European Parliament and of the Council of 17 April 2019 on the accessibility requirements for products and services (Text with EEA relevance), OJ L 151, 7.6.2019

Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, COM/2020/823 final

Proposal for a Directive of the European Parliament and the Council on the resilience of critical entities, COM/2020/829 final

Proposal for a regulation of the European Parliament and of the council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain Union legislative acts, COM(2021) 206 final

Proposal for a Regulation of the European Parliament and of the Council on machinery products, COM(2021) 202 final

Regulation (EC) No 1592/2002 of 15 July 2002

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) (Text with EEA relevance), *OJ L 119, 4.5.2016, p. 1–88.*

Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91.

Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union (Text with EEA relevance.), L 303/59

Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance), OJ L 151, 7.6.2019, p. 15–69

Other legislation

8 NOVEMBER 2020. - Koninklijk besluit tot uitvoering van uitvoeringsverordening (EU) 2019/947 van de Commissie van 24 mei 2019 inzake de regels en procedures voor de exploitatie van onbemande luchtvaartuigen [Dutch]

21 DECEMBER 2020. - Ministerieel besluit tot vaststelling van vaste geografische UAS-zones en toegangsvoorwaarden voor vaste geografische UAS-zones [Dutch]

Hellenic Supreme Court (Plen. Sess.) 1/2017, Hellenic Council of State 1616/2012, 2254/2005

Other sources

Agencia Española de Protección de Datos, ‘Drones and Data Protection’. 2019, [Online]. Available: https://www.aepd.es/sites/default/files/2019-09/guia-drones.pdf.

Citizen science Global. Available at: http://citizenscienceglobal.org/projects.html#his

ClientEarth, ‘Individual right to clean and healthy air in the EU’, p. 4, June 2021. https://www.clientearth.org/media/adtcznde/individual-right-to-clean-and-healthy-air-in-the-eu-pdf.pdf

CMS Germany, 'Scope of application of the e-privacy regulation', Available at: https://cms.law/en/deu/insight/e-privacy/scope-of-application-of-the-e-privacy-regulation

De Muyt, J.-P. "New EU drone rules What will change for everyone?", (2020, June 24). Consulted from https://euka.flandersmake.be/wp-content/uploads/2020/06/local-copy-EUKA-Session-June-24th.pd

De Smet, S., Free flow of non-personal data and GDPR, (2019, June 19). [Online]. Available : https://www.loyensloeff.com/en/en/news/news-articles/free-flow-of-non-personal-data-and-gdpr-n14929/

Droneguide, Available: https://map.droneguide.be]

DroneRules.eu, 'Privacy Handbook', [Online]. Available: https://dronerules.eu/assets/handbooks/PrivacyHandbook_EN.pdf

ECSA, 'ECSA's characteristics of citizen science'. (April 2020). Available : https://ecsa.citizen-science.net/wp-content/uploads/2020/05/ecsa_characteristics_of_citizen_science_-_v1_final.pdf

Electronic Privacy Information Center, 'EU Privacy and Electronic Communications (e-Privacy Directive)'. Available at : https://archive.epic.org/international/eu_privacy_and_electronic_comm.html

Evans, D. (2011), The Internet of Things: How the next evolution of the internet is changing everything, white paper 2, Cisco, San Jose, CA, available at http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

EU Monitor, 'Cybersecurity Act', Available at : https://www.eumonitor.nl/9353000/1/j9vvik7m1c3gyxp/vku7ds3xlvzx?ctx=vh6tfw7n7epz

GPDP, 'Consigli per rispettare la PRIVACY se si usa un DRONE a fini ricreativi', 2021, September. https://www.garanteprivacy.it/documents/10160/0/Utilizzo+di+droni+a+fini+ricreativi+e+privacy_+l%27infografica+del+Garante.pdf/482c901c-acc1-4aeb-9a9a-556376f84156?version=2.0

IPlens, A PROPOSAL FOR (AI) CHANGE? A succinct overview of the Proposal for Regulation laying down harmonised rules on Artificial Intelligence, 11 may 2021, *https://iplens.org/category/artificial-intelligence/*

Leslie, D., Burr, C., Aitken, M., Cowls, J., Katell, M., and Briggs, M. (2021). Artificial intelligence, human rights, democracy, and the rule of law: a primer. The Council of Europe. Available: https://www.turing.ac.uk/research/publications/ai-human-rights-democracy-and-rule-law-primer-prepared-council-europe

Modrall, J. (2021, April). *EU proposes new Artificial Intelligence Regulation*. Norton Rose Fulbright. https://www.nortonrosefulbright.com/en-gb/knowledge/publications/fdfc4c27/eu-to-propose-new-artificial-intelligence-regulation

Schouten, C. (n.d.). Marie Curie Individual Fellowship awarded to Anna Berti Suman, researcher on 'Citizen Sensing'. Tilburg University. https://www.tilburguniversity.edu/magazine/marie-curie-individual-fellowship-awarded-anna-berti-suman

The Soarizon Team, *'What are VLOS, EVLOS and BVLOS? Why do they affect drone operation?*, September 10, 2020. [Online]. Available: https://www.soarizon.io/news/what-are-vlos-evlos-and-bvlos-why-do-they-affect-drone-operations

UK Information Commissioner's Office, 'Drones'. [Online]. Available: https://ico.org.uk/your-data-matters/drones/