www.orchestra2020.eu

ORCHESTRA Project Deliverable: D1.3

Ethics, security, and gender balance plan

Authors: Anne Freiberger (IKEM), Anna-Lena Priebe (IKEM), Anna-Katharina Hübers (IKEM)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 953618. This document reflects only the author's view and the Agency is not responsible for any use that may be made of the information it contains.

About ORCHESTRA

The long-term vision of the ORCHESTRA is a future where it is easy to coordinate and synchronise the traffic management of all modes to cope with diverse demands and situations. Also, to facilitate optimal utilisation of transport networks and efficient multimodal transport services, both in rural and urban areas.

The project will:

- Establish a common understanding of multimodal traffic management concepts and solutions, within and across different modes, for various stakeholders and multiple contexts
- Define a Multimodal Traffic Management Ecosystem (MTME) where traffic managements in different modes and areas (rural and urban) are coordinated to contribute to a more balanced and resilient transport system, bridging current barriers and silos
- Support MTME realisation and deployments, through the provision of tools, models, and guidelines – including support for connected and automated vehicles and vessels (CAVs)
- Validate and adjust MTME for organisational issues, functionality, capability, and usability
- Maximise outreach and uptake of project results through strong stakeholder involvement

The project will provide a Polycentric Multimodal Architecture (PMA) that specify how diverse system components collaborate and interact, taking into account smart infrastructures, technical and organisational aspects and polycentric governance. The PMA will be supported by: 1) Enabling toolkit, 2) Deployment toolkit, 3) Documented lessons learned.

The project will validate the PMA and related tools and toolkits in two Living labs (in Norway and Italy), collectively covering both road, rail, water, and air transport. The Italian Living lab is focusing on traffic orchestration for the mobility of people, while the Norwegian Living lab is focusing on traffic orchestration for freight. The Living labs will be supported by simulations to enhance evaluations.

Legal disclaimer

Acknowledgment of EU funding

The project has received funding from the European Union's Horizon 2020 research and innovation program under Grant Agreement No 953618.

For more information

Project Coordinator: Runar Søråsen, runar.sorasen@its-norway.no

Dissemination Manager (WP7 leader): Jenny Simonsen, jenny.simonsen@its-norway.no

Executive Summary

The ethics, security and gender balance plan provides an overview of the ethical questions that arise through the implementation of the MTME concept in ORCHESTRA.

The ethical issues identified are subcategorised in different topics. The first topic covers **ethical issues of digitalisation**. These include potential data protection requirements, security requirements for MTMEs, the non-discriminatory use of digital tools, as well as responsibilities and liability issues deriving out of the automatization implemented in MTMEs.

The topic of non-discriminatory use of digital tools covers the description of digital tools, which will be developed during the project duration of ORCHESTRA. Furthermore, it provides the legal framework on discrimination and provides an assessment for the potential discrimination through the implemented digital tools. The recommendations describe to what extent technical developers need to pay attention for discriminative tendencies in regard of prioritising and the rewarding system on carbon credit allocation.

Moreover, the **social dimension of ORCHESTRA** is evaluated, which includes the risk of use of AI for employment and wages, as well as the risk of excluding transport solutions, and the gender dimension. The gender dimension of ORCHESTRA has multiple layers, as it must be taking into account internally within research teams, as well as for the concept of MTMEs, and throughout the involvement of research participants in living labs and the CoP.

Lastly, the ethical issues deriving out of the **CoP involvement** are addressed. Therefore, data protection requirements deriving out of the involvement of research participants are outlined. Concerning the issue of the protection of trade secrets of CoP members the overview of the legal framework on the protection of trade secret is provided. The advice is given to the consortium on how to inform CoP members on the topic of trade secrets prior to the involvement in research tasks is included.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 953618. This document reflects only the author's view and the Agency is not responsible for any use that may be made of the information it contains.

Table of Contents

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 953618. This document reflects only the author's view and the Agency is not responsible for any use that may be made of the information it contains.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 953618. This document reflects only the author's view and the Agency is not responsible for any use that may be made of the information it contains.

List of Abbreviations

Table 1: List of abbreviations

Abbreviation	Explanation
AI	Artificial intelligence
CAV	Connected and Automated Vehicles
CoP	Community of practitioners
ENISA	EU Agency for cybersecurity
ESGP	Ethics, security and gender balance plan
EU	European Union
EUCC scheme	Common Criteria based European candidate cybersecurity certification scheme
GDPR	General Data Protection Regulation
ITS	Intelligent transport systems
IXPs	Internet exchange points
MTM	Multimodal traffic management system
MTME	Multimodal Traffic Management Environment
NEC	Non-European Countries
NIS	Network and information security
PMA	Polycentric Multimodal Architecture
POPD	Protection of Personal Data
SAE	Society of Automotive Engineers
SOGIS-MRA	Senior Officials Group Information Systems Security Mutual Recognition Agreement
TOMs	Technical and organisational measures
TRIPS	Trade-Related Aspects of Intellectual Property Right
UDHR	Universal Declaration on Human Rights

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 953618. This document reflects only the author's view and the Agency is not responsible for any use that may be made of the information it contains.

1 About this Deliverable

1.1 Why would I want to read this deliverable?

This report covers ethical aspects of the research development processes in ORCHESTRA. It thereby focuses on the interaction between technical development of Multimodal Traffic Management Ecosystems (MTMEs) and potential ethical issues of digitalisation. Ethical and legal aspects of data protection, security as well as gender issues in relation to MTMEs will be explored.

D1.3 ensures awareness of ethical requirements throughout the technical development process from an early stage.

1.2 Intended readership/users

This report is addressed to all project partners of ORCHESTRA, who are involved in the conceptualisation and implementation of the MTME. The ethical, social and security dimensions of MTMEs need to be taken into account in order to derive at the best possible outcomes. In addition, the document is of value for all project partners who take part in research tasks, which involve CoP members.

Moreover, the document is useful for external technical developers in the digital traffic management and transport sector, as well as regulators who face similar relevant ethical and social questions, like the ones outlined. Furthermore, regulators working on the intersection between ethics and digitalisation might take the findings into account.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 953618. This document reflects only the author's view and the Agency is not responsible for any use that may be made of the information it contains.

2 Monitoring of ethics, security, and gender requirements

At the beginning of the monitoring process, relevant ethical issues regarding the conceptualisation and implementation of MTMEs have been addressed. The identification of the ethical issue was done in collaboration with the Innovation Manager of ORCHESTRA.

There are different types of ethical issue, which are of significance for the ORCHESTRA project. Some ethical issues arise in connection to the development process of MTMs as such. Moreover, other ethical dimensions arise internally from the gender dimension of the project, as well as the involvement of the CoP.

Article 19 Regulation (EU) No 1291/2013 on the establishment of H2020[1] establishes, that "all the research and innovation activities carried out under Horizon 2020 shall comply with ethical principles and relevant national, Union and international legislation, including the Charter of Fundamental Rights of the European Union and the European Convention on Human Rights and its Supplementary Protocols."

For OCHESTRA, the ethical and legal issues identified on this basis can be grouped into three different categories:

- **Ethical issues of digitalisation and autonomisation**
- **Social dimension of ORCHESTRA**
- **Ethical issues from CoP involvement**

The monitoring approach applied in ORCHESTRA by the LEPPI is to offer a dialogue towards upcoming ethical and legal issues with the consortium. Moreover, in cases where ethical and legal issues require specific tasks to be implemented by the project partners the necessary steps are communicated through the executive board meetings or workshop formats.

Furthermore, the Norwegian center for research data (NSD)[2] is involved as external experts on ethical and legal issue in the context of research data. The contact was established and is maintained by the project management of ORCHESTRA.

[1] Regulation (EU) No. 1291/2013 of the European Parliament and of the Council of 11 December 2013 establishing Horizon 2020 – the Framework Programme for Research and Innovation, available at: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:347:0104:0173:EN:PDF.

[2] Norwegian center for research data (NSD), https://www.nsd.no/en/.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 953618. This document reflects only the author's view and the Agency is not responsible for any use that may be made of the information it contains.

3 Ethical issues of digitalisation and automatisation

The topic of ethical issues of digitalisation and automatization requires special attention in regard to the development phase of MTMs in ORCHESTRA. Data protection requirements, security requirements, non-discriminatory use of technical tools, as well as responsibility and liability need to be taken into account.

3.1 Data protection requirements for MTMEs

In order to comply with the right to privacy enshrined in the EU Charter of Fundamental Rights[3] as well as the European Convention on Human Rights[4], the 2011 Transport White Paper issued by the European Commission states that the wider use of information technology tools will have to develop in parallel with the protection of privacy and personal data.[5] Since the latter is predominantly safeguarded by the General Data Protection Regulation (GDPR)[6], the following section will focus on the application and data protection requirements stipulated by the GDPR.

Scope of Application

According to Article 2 section 1 GDPR, the Regulation applies to the processing of data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

"Personal data" is defined in Article 4 section 1 GDPR and refers to any information relating to an identified or identifiable natural person, that is, a person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. While the concrete design of the MTME is yet to be realised, the current state of the ORCHESTRA project suggests that depending on the design of the tools used for the traffic management of passenger transports, the data involved could be potentially classified as personal data within the meaning of the GDPR. In the case of passenger transport, natural persons could register with applications administered by mobility service providers and thus share data such as their name, address, or date of birth with these actors. Moreover, in order for the application's algorithm to identify possible routes, individuals might have to enable it to track their location. However, findings indicate that the registration will be with application service providers, who will not share the personal data with stakeholders of the MTMs as such. This will depend on the actual data flows.

Freight transport often involve data attributable to a legal person and would, in such cases, not be protected by the GDPR. However, measures must be taken to protect information on the cargo types

[4] Convention for the Protection of Human Rights and Fundamental Freedoms [1950] ETS 5.

[5] European Commission, White Paper on Transport [2011] COM/2011/0144 final, para 47.

[6] 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 [2016] OJ L 119/1.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 953618. This document reflects only the author's view and the Agency is not responsible for any use that may be made of the information it contains.

and volumes transported to private persons, as information related to the addresses is personal data protected under the GDPR.

Moreover, personal data could also be inferred from connected and automated vehicles (CAVs). The latter refer to vehicles that use technologies to automate one or more elements of driving, resulting in different levels of driving automation.[7] While the degree of automation still needs to be specified in the context of ORCHESTRA, the Grant Agreement states that data will be collected from the CAVs' on-board sensors.[8] Therefore, in the case of passenger transport, the CAVs will potentially transfer location data, and the CAVs could be traced back to the car owner via the vehicle identification number and thus constitute personal data within the meaning of the GDPR. If the CAVs are used to provide transport services to travellers in general, the passengers may however not be known. In the case of freight transport, however, car owners tend to be legal persons whose data are not protected by the GDPR. If the CAV allows for the identification of the driver, for instance through digital driver cards, it could potentially collect personal data such as the name and address of the driver as a natural person. However, it seems unlikely that companies would transfer these data to the MTM system. Regarding the owner of CAV relevant authorities already have the information on personal or legal identity, as this is required in the admission process.

Consequently, the MTME could involve "personal data" within the meaning of the GDPR. In order to avoid data processing activities in the MTM system to be subject to GDPR thresholds, it is recommended to limit the use of personal data as far as technically possible.

"Processing", on the other hand, is defined by Article 4 section 2 GDPR and refers to any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. In order to facilitate multimodal transport management, personal data might be collected, evaluated and merged and thus "processed" within the meaning of the GDPR.

Lastly, according to Article 3 section 1 GDPR, the Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the EU. This will be the case for an MTME that depends on stakeholders based in the EU.

Anonymisation and Pseudonymisation

Depending on the final design of the MTME, personal data might be anonymised or pseudonymised before being inserted into the MTM system.

Anonymisation refers to the process of modifying personal data in a way that makes it impossible to allocate them to a specific data subject. Consequently, anonymised data can no longer be classified

[7] See, for instance, SAE International, Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles [2021] J3016_202104, available at https://www.sae.org/standards/content/j3016_202104/ [last accessed 08 September 2021].

[8] See, for instance, ORCHESTRA Grant Agreement, 953618, Part B p. 13.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 953618. This document reflects only the author's view and the Agency is not responsible for any use that may be made of the information it contains.

as personal data, which, according to Recital 26 GDPR, renders the data protection principles provided for by the GDPR inapplicable. The most prominent anonymisation techniques include randomisation, i.e. the alteration of the veracity of the data,[9] and generalisation, i.e. the dilution of the attributes of data subjects[10]. The safest method to fully anonymise personal data is considered to be the aggregation of data in order to form a data set that prevents individual data from being singled out and assigned to a specific person.[11] However, while Recital 26 GDPR states that in order to determine whether a natural person is identifiable, account should be taken of all the means likely to be used as well as of all objective factors, full anonymisation is hard to achieve in practice.[12]

Pseudonymisation, on the other hand, is not considered to be a method of anonymisation since it does not fully prevent the identification of a data subject.[13] According to Article 4 section 5 GDPR, pseudonymisation means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person. The process of pseudonymisation thus results in a data subject being replaced by indirect identifiers. However, pseudonymisation does not prevent the data from being classified as "personal" within the meaning of the GDPR.[14]

Whether or not the GDPR applies to data processed by the MTM system thus depends on whether the MTM system processes anonymised data. The latter, in turn, depends on the scope of the MTME, that is, if the MTME encompasses the collection of personal data or if it merely refers to the processing of data after having been collected and anonymised. In the case of ORCHESTRA, and according to the Grant Agreement, important stakeholders include local transport providers that offer relevant applications for end-users which depend on the collection of personal data prior to a potential anonymisation.[15] However, as mentioned earlier, it is recommended to limit the use of personal data as far as technically possible.

Lawfulness of Data Processing

Article 6 GDPR determines when the processing of personal data will be considered lawful.

In particular, according to Article 6 section 1 GDPR, processing shall be lawful if the data subject has given consent to the processing of his or her personal data for one or more specific purposes.

---

[9] Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques (0829/14/EN WP216), pages 12 – 16.

[10] Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques (0829/14/EN WP216), pages 16 – 19.

[11] Paal/Pauly/Ernst DS-GVO, Art. 4 para 49.

[12] Paal/Pauly/Ernst DS-GVO, Art. 4 Rn. 49.

[13] Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques (0829/14/EN WP216), page 3.

[14] Paal/Pauly/Ernst DS-GVO Art. 4 Rn. 49.

[15] ORCHESTRA Grant Agreement, 953618, Part B p. 7.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 953618. This document reflects only the author's view and the Agency is not responsible for any use that may be made of the information it contains.

Consent in that regard means any freely given, specific, informed, and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her pursuant to Article 4 section 11 GDPR. In the case of the MTME, end-users could give their consent to the processing of their personal data when agreeing to the terms and conditions of the relevant applications.

Article 7 GDPR determines the conditions for the processing of personal data based on consent. In particular, the controller shall be able to demonstrate that the data subject has consented to the processing of his or her personal data. Where the consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters in order for the declaration to be binding. The data subject shall also have the right to withdraw his or her consent at any time. However, in practice, data subjects might not always be able to accurately assess the scope of their consent, which leaves a residual risk with regard to the legal conformity of the particular declaration of consent.

Moreover, data processing is lawful pursuant to Article 6 section 1 GDPR if the processing is necessary for compliance with a legal obligation to which the controller is subject, in order to protect the vital interests of the data subject or of another natural person or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. Since the concrete design of the MTME is still to be discussed, it is questionable if one of these exemptions will apply in the context of ORCHESTRA.

Moreover, according to Article 9 section 1, the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation is prohibited. According to Article 9 section 2, this shall not apply if the data subject has given explicit consent to the processing. However, in the context of the MTME, it is unlikely that these data will be collected from natural persons.

Controllers and Processors in the Context of MTMEs

The GDPR sets out several responsibilities for the “controller” and the “processor”.

According to Article 4 section 7 GDPR, “controller” refers to the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data provided that this responsibility is not allocated by Union or Member State law. Consequently, controllers exercise decision-making power over the “why” and “how” of data processing.[16] Relevant factors to determine controllership in a given scenario include the data storage location and the de facto possibility to access the data.[17] Where two or more controllers jointly determine the purposes and means of processing, Article 26 GDPR determines that they shall be so-called joint controllers.

[16] European Data Protection Board, Guidelines 07/2020 on the concepts of controller and processor in the GDPR [2020] para 78.

[17] Paal/Pauly/Martini DS-GVO Art. 26 Rn. 19.

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 953618. This document reflects only the author’s view and the Agency is not responsible for any use that may be made of the information it contains.

The "processor", on the other hand, is defined by Article 4 section 8 GDPR as any natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller on the basis of a contract or other legal act within the meaning of Article 28 section 3 GDPR. Hence, processors do not exercise any independent control over the means of data processing but simply serve in the controller's interest, similar to the legal concept of delegation.[18]

The European Data Protection Board has recently issued a guideline on the meaning of controller and processor as stated in the GDPR.[19] According to this guideline, companies that disclose data to each other in order to carry out their respective services are each to be seen as individual controllers for the processing that they carry out within their services.[20] Similarly, where several entities use a common infrastructure or a shared database, they all act as individual controllers if each entity independently determines its own purposes in relation to the data that it feeds into the database.[21] However, if several institutions decide to participate in a joint project and use, to that end, the existing platform of one of these institutes, they all act as joint controllers.[22] On the contrary, where a company entrusts a cloud service provider with data management tasks but reserves the right to determine the purpose of data processing for itself, the company is to be seen as the controller and the cloud service provider as a mere processor.[23]

In the case of the MTME, several actors might qualify as (joint) controllers and processors within the meaning of the GDPR.

A first relevant actor is the local transport provider, a legal person, that collects personal data by way of an application installed on the end-users' phone. This actor collects data such as the name, birth date and address of end-users. Moreover, location data is collected in order to detect the possible routes available to the end-user. For the purpose of doing so, the local transport provider determines the purpose as well as the relevant means for collecting and evaluating the personal data and could, therefore, be seen as a "controller" within the meaning of the GDPR.

Another relevant actor is the legal person or authority responsible for the MTM system which receives location data from the application providers. This actor collects location data by end-users in order to facilitate comprehensive traffic management and, thus, for its own purpose. Consequently, this actor could also be labelled "controller" within the meaning of the GDPR. Moreover, depending on the final design of the MTM system, several legal persons or authorities could equally resume these responsibilities. Where these entities use a common infrastructure and do not individually decide on the purpose of the data used for traffic management, they could be seen as joint controllers.

Difficulties in determining the controller arise in the context of connected and automatic vehicles which might also play a role in the ORCHESTRA project. While the vehicle owner regularly lacks influence over the data processing, the manufacturer could take up the role of the controller if the

[18] European Data Protection Board, Guidelines 07/2020 on the concepts of controller and processor in the GDPR [2020] para 78.

[19] European Data Protection Board, Guidelines 07/2020 on the concepts of controller and processor in the GDPR [2020].

[20] ibid., para 90.

[21] ibid., para 69.

[22] ibid., para 66.

[23] ibid., para 82.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 953618. This document reflects only the author's view and the Agency is not responsible for any use that may be made of the information it contains.

data are transferred to a backend database or if the manufacturer is able to access the data remotely. Similarly, distributors and garages might access personal data during acquisition or maintenance services. Other relevant actors include mobility, infrastructure and telecommunication service providers. Where these actors are able to determine the purpose of data processing, they could all constitute individual "controllers" within the meaning of the GDPR as well.

Controller Responsibilities

The GDPR incorporates different responsibilities of the controller. In the case of joint controllers, Article 26 GDPR states that joint controllers shall in a transparent manner determine their respective responsibilities for compliance with the obligations under the GDPR, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14 GDPR, by means of an arrangement between them, provided that the latter is not determined by Union or Member State legislation. Consequently, if the MTME involves joint controllers within the meaning of the GDPR, their respective responsibilities and duties must be set out transparently in a respective contract.

According to Article 24 section 1 GDPR, the controller shall implement appropriate technical and organisational measures (TOMs) to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation, taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons. The provision thus serves as a general obligation to guarantee both data protection and data security by implementing the necessary technical and organisational safeguards.[24] When data collection occurs on behalf of the controller, the latter must ensure that the processor also implements the necessary TOMs pursuant to Article 38 section 1 GDPR.

In particular, with regard to data protection, TOMs must ensure the adherence to essential data-protection principles such as data minimisation which is stipulated by Article 25 sections 1 and 2 as well as Recital 156 GDPR. In addition to that, Recital 71 GDPR calls for technical and organisational measures to be implemented in order to minimise the risk of errors and prevent discriminatory effects. With regard to data security, Article 32 section 1 GDPR exemplifies the different forms of technical and organisation measures in the form of security measures. Appropriate TOMs include, but are not limited to, the pseudonymisation and encryption of personal data, the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services, the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident, a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing. The TOMs should be included in the record of processing activities as stipulated in Article 30 section 1 letter g and section 2 letter d GDPR.

Profiling and Automated Decision-Making

Special provisions on profiling and automated processing are enshrined in Articles 21 and 22 GDPR. Pursuant to Article 21 section 1 GDPR, the data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to the processing of their personal data which is based on Article 6 section 1 letters e or f GDPR, e.g. for tasks of public or other legitimate

[24] Paal/Pauly/Martini DS-GVO, Art. 32, Rn. 7.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 953618. This document reflects only the author's view and the Agency is not responsible for any use that may be made of the information it contains.

interest. This is especially the case for so-called data profiling. The latter is defined in Article 4 section 4 GDPR as any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Additionally, according to Article 22 section 1 GDPR, the data subject has the right not to be subject to a decision solely based on automated processing, including profiling as defined in Article 4 section 4 GDPR, which produces legal effects concerning him or her or similarly significantly affects him or her.

3.2 Security requirements for MTMEs

The 2011 Transport White Paper also states that the EU should strive for the universal application and enforcement of high standards of security in all modes of transport.[25] Since transport infrastructure is not limited to physical infrastructure but also involves large-scale intelligent and interoperable technologies[26], this cannot be interpreted restrictively but must be extended to data systems and digital mobility platforms such as the MTME.

3.2.1 General Data Protection Regulation

According to Article 24 section 1 GDPR, the controller shall implement appropriate technical and organisational measures (TOMs) to ensure and to be able to demonstrate that processing is performed in accordance with the Regulation, taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons. With regard to data security, Article 32 section 1 GDPR exemplifies the different forms of technical and organisation measures in the form of security measures. Appropriate TOMs include, but are not limited to, the pseudonymisation and encryption of personal data, the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services, the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident, a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

3.2.2 NIS Directive

The so-called NIS Directive[27] seeks to achieve a high common level of security of network and information systems in the Union in order to improve the functioning of the internal market. To this end, each Member State ought to adopt a national strategy on the security of network and information systems[28] which is monitored by a so-called Cooperation Group[29].

MTMEs as operator of essential services

[25] European Commission, White Paper on Transport [2011] COM/2011/0144 final, para 29.
[26] ibid., para 43.
[27] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union [2016] OJ L 194/1.
[28] NIS Directive, Article 7 and following.
[29] NIS Directive, Article 11 and following.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 953618. This document reflects only the author's view and the Agency is not responsible for any use that may be made of the information it contains.

According to its Article 5 section 1, Member States must identify the "operators of essential services" with an establishment on their territory. The term "operators of essential services" is defined in Article 4 section 4 NIS Directive. It refers to any public or private entity of a type referred to in Annex II which meets the criteria laid down in Article 5 section 2 NIS Directive.
Annex II of the NIS Directive lists, inter alia, the transport sector, which is then subdivided into air, rail, water, and road transport. While multimodal traffic management is not explicitly mentioned as an overall category, several of the subcategories contain references to intelligent transport management. For instance, the air transport category mentions airport managing bodies as defined in Article 2 of Directive 2009/12/EC[30], that is, bodies that are responsible for the administration and management of the airport or airport network infrastructures and the coordination and control of the activities of the different operators present in the airports or airport network concerned. Moreover, the air transport category lists traffic management control operators providing air traffic control as defined in Article 2 section 1 of Regulation (EC) 549/2004[31], i.e., services provided for the purposes of preventing collisions between aircraft and in the manoeuvring area between aircraft and obstructions as well as expediting and maintaining an orderly flow of air traffic. Similar examples are listed in the rail, water and road transport subcategories. For instance, the rail transport category mentions infrastructure managers as defined in Article 3 point 2 of Directive 2012/34/EU[32], that is, bodies or firms responsible in particular for establishing, managing and maintaining railway infrastructure, including traffic management. Most importantly, however, is the reference to operators of intelligent transport systems (ITS) as defined in Article 4 point 1 of Directive 2010/40/EU[33]. According to this provision, ITS means systems in which information and communication technologies are applied in the field of road transport, including infrastructure, vehicles, and users, and in traffic management and mobility management, as well as for interfaces with other modes of transport. Consequently, while the specific tasks of the MTM system are yet to be devised, it is likely that it falls within the ambit of Article II of the NIS Directive.

Annex II of the NIS Directive also mentions digital infrastructure as a category. However, the latter is only subdivided into internet exchange points (IXPs), DNS service providers and TLD name registries. The MTM system does not provide for any of these services.

Article 5 section 2 NIS Directive lays down four criteria for the identification of the operators of essential services. Firstly, the entity must provide a service which is essential for the maintenance of critical and societal and/or economic activities. If the MTM system's task is to manage traffic flows across modes, this service can be deemed as the very basis for the continuation of the large-scale societal and economic activities envisaged by the MTME. However, one could also argue that the MTM system merely optimizes traffic as a whole but does not constitute a necessary component of the traffic system. Secondly, the provision of that service must depend on network and information

[30] Directive 2009/12/EC of the European Parliament and of the Council of 11 March 2009 on airport charges [2009] OJ L 70/11.
[31] Regulation (EC) No 549/2004 of the European Parliament and of the Council of 10 March 2004 laying down the framework for the creation of the single European sky [2004] OJ L 96/1.
[32] Directive 2012/34/EU of the European Parliament and of the Council of 21 November 2012 establishing a single European railway area [2012] OJ L 343/32.
[33] Directive 2010/40/EU of the European Parliament and of the Council of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport [2010] OJ L 207/1.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 953618. This document reflects only the author's view and the Agency is not responsible for any use that may be made of the information it contains.

systems. This is naturally the case for an MTM system that operates through digital platforms. Lastly, an incident must have significant disruptive effects on the provision of that service. "Incident" is defined in Article 2 section 7 as any event having an actual adverse effect on the security of network and information systems. In case the MTM's digital platforms and data flows are severely affected, traffic management through the tools will presumably no longer be possible, which, in turn, would result in significant disruptive effects on the traffic flows covered by the system.

According to Article 14 NIS Directive, Member States need to ensure that operators of essential services take appropriate and proportionate technical and organizational measures to manage the risks posed to the security of network and information systems which they use in their operations.[34] Similar measures should be taken for the prevention and minimization of incidents as defined above.[35]

MTM as a digital service provider

Pursuant to Article 16 section 1 NIS Directive, Member States ought to ensure that "digital service providers" identify and take appropriate and proportionate technical and organizational measures to manage the risks posed to the security of network and information systems. The term "digital service" is defined in Article 4 section 5 NIS Directive and refers to a service within the meaning of Article 1 section 1 point b of Directive 2015/1535/EU[36] which is of a type listed in Annex III NIS Directive. The latter merely refers to three types of digital services, i.e., online marketplace, online search engine, and cloud computing service. While the specific tasks of the MTM system are yet to be devised, an MTME does not involve any of the services listed in Annex III NIS Directive and does not, therefore, constitute a digital service provider within the meaning of the NIS Directive.

3.2.3 Reform of the NIS Directive

In December 2020, the European Commission adopted its so-called Cybersecurity Strategy for the Digital Decade.[37] The latter seeks to strengthen the EU's collective defences against cyber threats in order to ensure a global and open Internet and safeguard the security and fundamental rights and freedoms of people in Europe. To this end, regulatory, investment and policy instruments in three areas of EU action (area of resilience, technological independence and leadership, all Internet-connected things in the EU; building operational capacity for prevention, deterrence and response; and promoting a global open cyberspace) will be deployed.
One of these instruments is the revised NIS-2 Directive as proposed by the Commission in December 2020.[38] The latter is intended to modernize the existing legal framework provided by the NIS Directive by expanding its scope but at the same time tightening up several requirements,

[34] NIS Directive, Article 14 section 1.
[35] NIS Directive, Article 14 section 2.
[36] Directive (EU) 2015/1535 of the European Parliament and of the council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services.
[37] European Commission, Joint Communication to the European Parliament and the Council - The EU's Cybersecurity Strategy for the Digital Decade [2020] JOIN/2020/18 final.
[38] European Commission, 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 [2020] COM/2020/823 final.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 953618. This document reflects only the author's view and the Agency is not responsible for any use that may be made of the information it contains.

benchmarks as well as control and sanction options. To this end, the proposal adds new sectors[39] and a size-cap rule whereby all medium and large enterprises that operate within these sectors or provide the type of services fall within its scope.[40] Moreover, the distinction between "operators of essential services" and "providers of digital services" is eliminated. Instead, the proposal distinguishes between "essential" and "important" entities.[41] According to Article 4 section 25 NIS-2 Directive, “essential entity” means any entity of a type referred to as such in Annex I. Similar to the current NIS Directive, Annex I mentions the category of “transport” and subdivides it into air, rail, water and road, while referring to the service providers mentioned earlier. Furthermore, pursuant to Article 4 section 26 NIS-2 Directive, “important entity” means any entity of a type referred to as such in Annex II. The latter adds several sectors to the scope of the NIS-2 Directive, however, none of them seem to encompass an MTME.

In addition to that, the proposal expands the definition of "security incident". Under the NIS-2 Directive, any event compromising the availability, authenticity, integrity, or confidentiality of stored, transmitted or processed data or of the related services offered by, or accessible via, network and information systems will suffice.[42]
Lastly, the necessary security measures that have to be introduced by essential and important entities are specified.[43] For instance, Article 18 section 2 letter g of the proposal encourages the use of cryptography and encryption. The respective entities should also engage in an exchange of relevant cybersecurity information among themselves.[44]
More detailed information on the topic will further be included in D2.2 Pre-Studies on environment analysis and drivers, which focuses on the ethical and legal framework on MTMEs.

3.2.4 Cybersecurity Act and EUCC scheme

The so-called Cybersecurity Act[45], and EU Regulation, seeks to strengthen the role of the EU Agency for cybersecurity (ENISA) and to establish a cybersecurity certification scheme. The latter will replace the existing schemes operating under the SOG-IS MRA.[46] To this end, it will provide for an EU-wide comprehensive set of rules, technical requirements and procedures and attest that network or information system products, services and processes comply with specified security requirements.[47] These requirements vary depending on the level of risk associated with the intended

[39] ibid., Recital 11.
[40] ibid., Recital 8.
[41] ibid., Recital 11.
[42] ibid., Article 4 section 5.
[43] ibid., Article 18.
[44] Commission proposal, Article 26.
[45] 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 [2019] OJ L 151/15.
[46] Senior Officials Group Information Systems Security (SOG-IS), Mutual Recognition Agreement of Information Technology Security Certificates [2010]. See also the Statement of the SOG-IS Management Committee on the relation between the SOG-IS Agreement and the European Certification Framework that is under negotiation at the EU Commission, available at https://www.sogis.eu/documents/mra/201802-SOGIS-Position.pdf [last accessed 08 September 2021].
[47] Cybersecurity Act, Article 46 and following.

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 953618. This document reflects only the author’s view and the Agency is not responsible for any use that may be made of the information it contains.

use of those products, services and processes and thus classified into "basic", "substantial" and "high" assurance levels.[48] Moreover, Article 54 Cybersecurity Act contains minimum requirements of EU cybersecurity certification schemes, for instance, the subject matter and scope, a clear description of the purpose, the assurance level and the evaluation criteria. The resulting certificate will be recognised in all EU Member States.[49]

In May 2021, ENISA has published the Common Criteria based European candidate cybersecurity certification scheme (EUCC scheme).[50]

3.3 Responsibility and liability issues of automatization in MTMEs

As MTMEs will include automatization within its scope, responsibility and liability issues may arise. These should be taken into account by the ORCHESTRA consortium in all stages of the research process.

In particular, traffic management will predominantly be carried out by automated digital tools.[51] The latter refers to the technical implementations, i.e., processing systems, programs, services, platforms or software characterized by electronic or computerized technologies, that facilitate the realisation and deployment of the MTM.[52]

Moreover, the MTME relies on smart infrastructure to fully integrate connected and automated vehicles (CAVs) into the ecosystem.[53]

3.3.1 Legal responsibility and liability issues in highly automated systems

CAVs are vehicles and vessels that use technologies to automate one or more elements of driving. According to the widely accepted SAE International (formerly Society of Automotive Engineers) classification scheme for CAVs on road, six levels of driving automation can be distinguished.[54] While levels zero to two merely involve driver support features such as brake or acceleration support, levels three and four refer to automated driving features which can drive the vehicle under certain conditions. Finally, level five vehicles can drive everywhere in all conditions and thus constitute fully autonomous cars. While the degree of automation still needs to be specified in the context of the ORCHESTRA project, the Grant Agreement leaves room to eventually encompass even fully autonomous cars.[55]

Autonomous systems are also entirely dependent on artificial intelligence (AI). The latter refers to the digital imitation of intelligent human behaviour and encompasses, inter alia, machine-learning algorithms which act independently from any human intervention since they are able to constantly

[48] Cybersecurity Act, Article 52 section 1.
[49] Cybersecurity Act, Article 56 section 1.
[50] See ENISA, Cybersecurity Certification: Candidate EUCC Scheme V1.1.1 [2021], available at Cybersecurity Certification: Candidate EUCC Scheme V1.1.1 — ENISA (europa.eu)
[51] See ORCHESTRA Grant Agreement, 953618, Part B p. 14.
[52] ibid., p. 14 f.
[53] ibid., p. 14.
[54] See, for instance, the widely accepted classification by SAE International, Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles [2021] J3016_202104, available at https://www.sae.org/standards/content/j3016_202104/.
[55] The ORCHESTRA Grant Agreement simply states, for instance, that data will be collected from CAV's on-board sensors, see ORCHESTRA Grant Agreement, 953618, Part B p. 13.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 953618. This document reflects only the author's view and the Agency is not responsible for any use that may be made of the information it contains.

adjust their own tasks by evaluating prior experience.[56] CAVs, for instance, rely on AI machine-learning algorithms that collect data inferred from advanced sensory systems providing 360-degree information on the vehicle's environment, identify locations, plan and follow routes and recognise obstacles. In the case of level three automated vehicles and beyond, AI will have full control over the vehicle at least for some time.[57]

Since decision-making is increasingly carried out semi or fully automatically, it becomes increasingly difficult to determine who is responsible for the system's actions, potentially resulting in the emergence of so-called responsibility gaps.[58] Responsibility can generally be understood in different ways. While "forward-looking" responsibility is primarily concerned with mitigating risks and avoiding future harm, "backward-looking" responsibility determines who will be held responsible for things that happened in the past. The latter can, in turn, be understood as moral culpability, accountability or legal liability.[59]

Accountability as understood by the European Commission refers to the obligation to explain that something has happened and which role one plays in its occurrence. Hence, the relevant persons or institutions should be able to explain each action carried out by the respective automated system.[60] Since the final design of the MTME is yet to be realised, it is still unclear who could be held accountable for automated decision-making in the context of ORCHESTRA. However, accountability as understood in this Deliverable should be kept in mind when distributing the tasks relating to any automated system.

Legal liability, on the other hand, particularly refers to criminal and civil liability of individuals or institutions. The issue of civil liability for damage occurred by automated decision-making is important for ORCHESTRA. Most legal systems in the EU distinguish between contractual and extra-contractual liability (also called "tort"), i.e., where liabilities are set without the existence of a contract. The default principle in all EU member states is fault-based liability, which determines whether the party in question negligently or deliberately violated an obligation corresponding to him or her in order to compensate the party who suffered a loss.[61] In the context of automated systems, however, the average person might behave completely in accordance with their duties and have no corresponding risk knowledge, resulting in a situation where a party could not be

[56] European Commission, Algorithmic discrimination in Europe - Challenges and opportunities for gender equality and non-discrimination law, available at https://www.equalitylaw.eu/download s/5361-algorithmic-discrimination-in-europe-pdf-1-975, p. 33.

[57] Council of Europe, Committee on Legal Affairs and Human Rights, Report on legal aspects of "autonomous" vehicles [2020], available at https://assembly.coe.int/LifeRay/JUR/Pdf/DocsAndDecs/2020/AS-JUR-2020-20-EN.pdf, no. 8.

[58] See for this term European Commission, Ethics of Connected and Automated Vehicles - Recommendations on road safety, privacy, fairness, explainability and responsibility [2020], available at https://op.europa.eu/en/publication-detail/-/publication/89624e2c-f98c-11ea-b44f-01aa75ed71a1/language-en/format-PDF/source-search [last accessed 14 September 2021] p. 53; Council of Europe, Committee on Legal Affairs and Human Rights, Report on legal aspects of "autonomous" vehicles [2020], available at https://assembly.coe.int/LifeRay/JUR/Pdf/DocsAndDecs/2020/AS-JUR-2020-20-EN.pdf, no. 2.

[59] See for that distinction European Commission, Ethics of Connected and Automated Vehicles - Recommendations on road safety, privacy, fairness, explainability and responsibility [2020], available at https://op.europa.eu/en/publication-detail/-/publication/89624e2c-f98c-11ea-b44f-01aa75ed71a1/language-en/format-PDF/source-search, p. 54.

[60] ibid., p. 58.

[61] Herbert Zech, Liability for AI: Public Policy Considerations (ERA Forum 2021, 22: 147), page 151.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 953618. This document reflects only the author's view and the Agency is not responsible for any use that may be made of the information it contains.

compensated for the damage incurred.[62] In the face of these consequences, some states have also opted for strict liability rules, especially in the case of road traffic.[63]

On an EU level, Directive 85/374 on the Liability for Defective Products[64] sets out rules on the (strict) liability of producers and the rights of consumers. However, this Directive is not applicable where the product is not considered to be defective within the meaning of the Directive, which might be the case for semi or fully autonomous systems that decide on their actions independently from any human intervention.[65] Therefore, in December 2020, the European Parliament requested the European Commission to submit a proposal for a regulation on a civil liability regime for artificial intelligence.[66] In response to this, the European Commission is currently carrying out an inception impact assessment for a future legislative proposal titled ”Adapting liability rules to the digital age and circular economy”.[67] The proposal will presumably be adopted in the third quarter of 2022.[68]

At the moment, EU Member States' legislative regimes are still diverse and not fully embracing current developments in the field of automation. It is thus important to closely monitor legal discussions on the reform of liability allocated for automated decision-making.[69]

3.3.2 Trust in autonomous technologies (CAV, drones, etc.)

The increasing introduction of autonomous technologies into society, the workplace, and the economy is considered to be one of the most important issues on the current political agenda.[70] However, in light of these ever-improving technological innovations, it seems questionable on what basis individual members of society value technological advances, or, put simply, if they trust new technologies involving autonomous decision-making. In the context of ORCHESTRA, this is particularly important with regard to connected and automated vehicles (CAVs).

In sociological research, trust in automation is commonly defined as “the attitude that an agent will help achieve an individual's goals in a situation characterized by uncertainty and vulnerability”.[71] In

[62] Council of Europe, Committee on Legal Affairs and Human Rights, Report on legal aspects of “autonomous” vehicles [2020], available at https://assembly.coe.int/LifeRay/JUR/Pdf/DocsAndDecs/2020/AS-JUR-2020-20-EN.pdf., 28.
[63] See, for instance, section 7 of the German Road Traffic Act.
[64] Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products [1985] OJ L 210/29.
[65] See Council of Europe, Committee on Legal Affairs and Human Rights, Report on legal aspects of “autonomous” vehicles [2020], available at https://assembly.coe.int/LifeRay/JUR/Pdf/DocsAndDecs/2020/AS-JUR-2020-20-EN.pdf, no. 42.
[66] European Parliament, Resolution of 20 October 2020 with Recommendations to the Commission on a Civil Liability Regime for Artificial Intelligence [2020] 2020/2014/INL.
[67] European Commission, Adapting liability rules to the digital age and circular economy [2021] Ref. Ares(2021)4266516 - 30/06/2021, available at https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12979-Civil-liability-adapting-liability-rules-to-the-digital-age-and-artificial-intelligence_en.
[68] See ibid.
[69] See, for instance, Horst Eidenmüller, The Rise of Robots and the Law of Humans (ZEuP 2017, 765); Herbert Zech, Liability for AI: Public Policy Considerations (ERA Forum 2021, 22: 147).
[70] See European Parliament, Resolution of 20 October 2020 with Recommendations to the Commission on a Civil Liability Regime for Artificial Intelligence [2020] 2020/2014/INL, Introduction no 1.
[71] Kaspar Raars, Vaike Fors, Sarah Pink, Trusting autonomous vehicles: An interdisciplinary approach [2020] Transportation Research Interdisciplinary Perspectives, Volume 7, p. 2.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 953618. This document reflects only the author's view and the Agency is not responsible for any use that may be made of the information it contains.

this regard, the European Commission has identified trustworthiness of digital technologies as a cornerstone of their acceptance in the EU.[72] Hence, it has not only continuously emphasized that developing and implementing trustworthy artificial intelligence is on the forefront of its political agenda[73], but has identified the creation of a so-called ”ecosystem of trust” as a policy objective in itself[74]. To achieve that goal, the European Commission has outlined three basic components: artificial intelligence should comply with the law, fulfil ethical principles and be robust. Based on these components, AI applications should fulfil seven key requirements in order to be considered trustworthy, namely human agency and oversight, technical robustness and safety, privacy and data governance, transparency, diversity, non-discrimination and fairness, societal and environmental well-being and accountability.[75] In its 2021 inception impact assessment for a proposal on liability within the realm of AI systems, the Commission particularly called for enhanced liability rules in order to build trust by providing effective redress to injured parties.[76]

In light of these developments, any autonomous technologies implemented in the context of the ORCHESTRA project should adhere to the principles outlined by the Commission in order to ensure that individuals trust and use them accordingly.

3.4 Non-discriminatory use of digital tools

The non-discriminatory use of technical tools is needed in order to be in line with ethical and legal requirements. Therefore, the digital tools, which will be developed in the designing phase of ORCHESTRA will be further analysed.

3.4.1 Digital tools in the ORCHESTRA project

Prior to identifying any discriminatory practices that the implementation of digital tools in the course of the ORCHESTRA project is likely to bring about, the relevant concepts need to be defined. “Digital tools” in the ORCHESTRA project refers to the technical implementations, i.e. processing systems, programs, services, platforms or software characterized by electronic or

[72] European Commission, White Paper on Artificial Intelligence - A European approach to excellence and trust [2020] COM(2020) 65 final, available at https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf p. 1.

[73] See, for instance, European Commission, Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions: Fostering a European approach to Artificial Intelligence, Annex: Coordinated Plan on Artificial Intelligence 2021 Review [2021] COM(2021) 205 final, p. 2, available at file:///C:/Users/Anna-LenaPriebe/Downloads/1_en_annexe_autre_acte_part1_v8_vf_C4B261EB-ABA4-5C30-1555482869410384_75787%20(1).pdf.

[74] European Commission, White Paper on Artificial Intelligence - A European approach to excellence and trust [2020] COM(2020) 65 final, available at https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf p. 3.

[75] European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – Building Trust in Human-Centric Artificial Intelligence [2019] COM(2019) 168 final, available at file:///C:/Users/Anna-LenaPriebe/Downloads/1_en_act_part1_v8_DA596EE2-A7B1-2FF2-976724FBD96DE1F1_58496.pdf, p. 3.

[76] European Commission, Adapting liability rules to the digital age and circular economy [2021] Ref. Ares(2021)4266516 - 30/06/2021, available at https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12979-Civil-liability-adapting-liability-rules-to-the-digital-age-and-artificial-intelligence_en, p. 5.

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 953618. This document reflects only the author’s view and the Agency is not responsible for any use that may be made of the information it contains.

computerized technologies, that facilitate the realisation and deployment of the multimodal traffic management system (MTM). This particularly includes tools for the automatic collection of data from different stakeholders that will be merged and serve as inputs for dynamic transport demand management tools and demand capacity balancing tools. The tools provide for access control, priorities and reward of desired behaviour as well as re-planning indications and speed adjustments. Moreover, if a conflict is detected, a digital arbitration tool will engage in decision support and prioritisation based on the inputs inferred from the other tools.[77] In order to fulfil their purpose, the MTM will heavily rely on algorithms.[78] The latter can be defined as "basic, formalised and precisely defined computation rules or rules for a sequence of computation steps that are set up to execute a given task."[79] They are implemented and programmed in a programming language (e.g. Python) and must be supplied with inputs in order to generate an output, both usually in the form of data.[80] Inputs can be provided manually by humans and machines, or, as technology advances, by the algorithm itself whenever it falls within the realm of artificial intelligence. The latter refers to the digital imitation of intelligent human behaviour and encompasses, inter alia, machine-learning algorithms which act independently from any human intervention since they are able to constantly adjust their own tasks by evaluating prior experience.[81] If these algorithms are trained with unlabelled data, thereby autonomously processing data, discovering correlations and establishing new links based on those data, they are referred to as "black-box" algorithms which eventually become unreadable to their designers.[82] In recent years, algorithm-based analysis methods have evolved significantly. They include, for instance, data mining (i.e., the identification of statistical correlations in data sets) and so-called "big data" analytics (i.e., the automated collection, processing, and analysis of large data sets). Other common areas of application are profiling, which refers to the processing of data to create and update a comprehensive record of data subjects, and scoring, which involves the assignment of numerical values to a data subject on a scale. Lastly, the aforementioned techniques enable so-called data forecasts, i.e., the calculation of probabilities, thereby usually classifying data subjects into classes on the basis of a differentiation criteria.[83] In the ORCHESTRA project, as described above, algorithms will engage in the collection, merger and analysis of data from different stakeholders as well as data forecasts by calculating transport probabilities. Moreover, based on the collected data, priorities will be allocated, and desired behaviour rewarded, which might amount to data profiling and data scoring.[84]

[77] ORCHESTRA Grant Agreement 953618, Part B, p. 14 f.
[78] ibid., p. 20.
[79] Carsten Orwat on behalf of the German Federal Anti-Discrimination Agency, Risks of Discrimination through the Use of Algorithms, p. 11.
[80] ibid., p. 11.
[81] European Commission, Algorithmic discrimination in Europe - Challenges and opportunities for gender equality and non-discrimination law, available at https://www.equalitylaw.eu/download s/5361-algorithmic-discrimination-in-europe-pdf-1-975, p. 33.
[82] ibid., p. 35.
[83] Carsten Orwat on behalf of the German Federal Anti-Discriminatio n Agency, Risks of Discrimination through the Use of Algorithms, p. 15.
[84] ibid., p. 20 – 21; 145 ff.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 953618. This document reflects only the author's view and the Agency is not responsible for any use that may be made of the information it contains.

3.4.2 Legal framework on discrimination

Both international and national law contain provisions ensuring equality and prohibiting discrimination based on different characteristics. On an international level, Article 1 and 2 of the Universal Declaration on Human Rights (UDHR) safeguard the principle of equality, stating that all human beings are born equal in dignity and rights[85] and that, therefore, everyone is entitled to all the rights set forth in the UDHR without distinction of any kind, such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status86. Article 7 UDHR adds that all human beings are equal before the law, entitled without discrimination to equal protection of the law as well as to equal protection against any discrimination in violation of the UDHR or incitement to such discrimination. Similarly, on an EU level, Article 2 TEU stipulates that the EU is founded on the values of, inter alia, equality and respect for human rights, amounting to a society in which non-discrimination prevails. According to Article 3 section 3 TEU, the Union shall therefore combat discrimination. Likewise, Article 10 TFEU sets forth that the EU shall aim to combat discrimination based on sex, racial or ethnic origin, religion or belief, disability, age or sexual orientation. Moreover, within the scope of the Treaties, any discrimination on grounds of nationality is prohibited pursuant to Article 18 TFEU. A similar prohibition is enshrined in Article 21 of the EU Charter of Fundamental Rights.[87] Finally, national laws proscribe the discrimination based on different characteristics.[88]

Special provisions on non-discrimination are also enshrined in the GDPR. Recital 71 GDPR states that the controller should secure personal data in a way that prevents discriminatory effects on natural persons on the basis of racial or ethnic origin, political opinion, religion or beliefs, trade union membership, genetic or health status or sexual orientation, or that result in measures having such an effect. Moreover, according to Article 9 GDPR, processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall generally be prohibited. Further provisions on profiling and automated processing are enshrined in Articles 21 and 22 GDPR. Pursuant to Article 21 section 1 GDPR, the data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to the processing of their personal data which is based on Article 6 section 1 letters e or f GDPR, e.g. for tasks of public or other legitimate interest. This is especially the case for so-called data profiling. The latter is defined in Article 4 section 4 GDPR as any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Additionally, according to Article 22 section 1 GDPR, the data subject has the right not to be subject to a decision solely based on automated processing, including profiling as defined in Article 4 section 4 GDPR, which produces legal effects concerning him or her or similarly significantly affects him or her.

[85] UDHR, Article 1 Sentence 1.
[86] UDHR, Article 2 Sentence 1.
[87] See on the interplay between algorithms and the Charter Council of the European Union, Presidency conclusions - The Charter of Fundamental Rights in the context of Artificial Intelligence and Digital Change [2020] 11481/20.
[88] See, for instance, Article 3 of the German Basic Law and the German General Equal Treatment Act.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 953618. This document reflects only the author's view and the Agency is not responsible for any use that may be made of the information it contains.

With regard to AI, the European Commission, several key EU actors have expressed concerns over algorithmic discrimination.[89] In light of these developments, the European Commission has reviewed its 2018 Coordinated Plan on Artificial Intelligence[90] and highlighted the importance of non-discriminatory AI algorithms particularly in the field of multi-modal transport. Moreover, it has adopted a proposal for a regulation on artificial intelligence[91] that could eventually bring about further specifications on the avoidance of algorithmic discrimination, in particular with regard to the data sets deployed for the development of AI systems and ongoing obligations for testing, risk management, documentation and human oversight.[92]

3.4.3 Potential discrimination through ORCHESTRA's digital tools

Since the MTM system is instructed to gather data from different stakeholders in order to reconcile both the different means of transportation and passengers and engage in independent decision-making as described earlier, discrimination via digital tools during the ORCHESTRA project might potentially occur in various situations. However, technical tools and the algorithms need to be distinguished to the extent that they will process data themselves, or merely help to validate the identity of specific attributes.

Scenario 1: Prioritisation

In particular, the MTM system might facilitate indirect discrimination where location data allow for further conclusions and where the algorithm's decision-making process is based on criteria that result in the disadvantageous treatment of individuals merely because of their given location. This is especially the case where the MTM algorithm is obliged to allocate resources that are limited in terms of time, space, or personnel. In that case, the MTM's algorithm will determine priorities. According to the ORCHESTRA Grant Agreement, a network user will be prioritised if their transport operation is time critical or "considered more important than other operations".[93]

The negotiation process of prioritisation purposes is still not developed under the current stage of the project. The deciding factors on how the negotiation process will come to conclusions is yet to be designed. However, a different output might be obtained with the same input, if the negotiation scheme is designed differently.

---

[89] See, for instance, European Parliament, Resolution with recommendations to the Commission on a framework of ethical aspects of artificial intelligence, robotics and related technologies [2020] 2020/2012(INL); Council of the European Union, Presidency conclusions - The Charter of Fundamental Rights in the context of Artificial Intelligence and Digital Change [2020] 11481/20.

[90] European Commission, Communication from the Commission - Coordinated Plan on Artificial Intelligence [2018] COM/2018/795 final.

[91] 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 [2021] COM/2021/206 final.

[92] ibid., 1.2; Recitals 10, 13, 15, 17, 28, 33, 35, 36, 37, 38, 39, 44, 45, 47.

[93] ORCHESTRA Grant Agreement 953618, Part B, p. 15: "Priorities. Network users may get priorities if their transport operation is time critical or considered more important than other operations. Certain requirements may have to be fulfilled (e.g. green vehicle), Credentials must ensure the right decisions."

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 953618. This document reflects only the author's view and the Agency is not responsible for any use that may be made of the information it contains.

Discrimination might also occur where a person has selected specific options in their digital user profile, such as special needs that require transport designed to fit those needs as well as gender related aspects.[94] Naturally, the algorithm that selects the suitable transport options for this person must take these preferences into account. However, if a person subsequently prefers one of the options presented to him or her on a regular basis, the algorithm could interpret their regular choice as a general tendency for individuals that have selected the same preference and automatically exclude other options. For instance, if different transport options are presented to a female traveller who seeks to travel at night, and she regularly chooses the shortest option, the algorithm could infer from that choice that female travellers will always choose that option. This might result in the algorithm not displaying other (perhaps cheaper or more suitable) options based on the person's gender.

Scenario 2: Rewarding and Punishment

According to the ORCHESTRA Grant Agreement, one of the digital tools will establish the reward of desired behaviour as well as the punishment of undesired behaviour.[95] Desired behaviour will include the use of green modes and avoidance of using networks during rush hours, for which users are credited and will get advantages such as carbon credits.[96]

However, the determination of what constitutes desired and undesired behaviour might facilitate discrimination where the choice of the behaviour in question is by itself discriminatory. Since the MTM system solely processes travellers' location data, this could be the case where the behaviour is linked to the person's location. For instance, carbon credits will presumably be allocated to travellers who prefer the greener, but longer ride, as opposed to travellers who will take the faster means of transport. However, if a person lives on the outskirts of the city, he or she might be more dependent on faster means of transport than persons living closer to the city centre. If the outskirts are predominantly inhabited by a group that falls within the characteristics defined above, such as persons of a certain ethnic origin, this could result in the unequal treatment of those persons.

Another discriminatory situation could occur where the rewarded or punished behaviour is linked to the person's digital profile preferences. Direct discrimination could take place if a person were punished or denied advantages simply because of her personal preferences that fall within the realm of the characteristics defined above (e.g., gender or disability). Moreover, if greener modes of travel are generally more expensive than other means of transport, individuals with a lower income might simply not be able to afford green transport as frequently as individuals with a higher income. However, privileging individuals with a higher income reflects a wider social issue that calls for social policy adaptations rather than a solution tailored to the users in the ORCHESTRA ecosystem.

3.4.4 Recommendations

As a consequence of the potential discrimination resulting from the MTM system, technical developers need to pay close attention to discriminative tendencies when designing the digital tools and negotiation schemes, both with regard to prioritisation and the reward system through carbon credit allocation. In particular, the inputs and decision-making rules for algorithms need to be

[94] ibid., Part B, p. 8 footnote 5.
[95] ibid., Part B, p. 15.
[96] ibid., Part B, p. 14 – 15.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 953618. This document reflects only the author's view and the Agency is not responsible for any use that may be made of the information it contains.

constructed in a way that avoids the reproduction of biases and prejudices. Data need to be accurate, updated and not influenced by under- or overrepresentation of certain groups. It should be noticed that the examination of discriminatory effects of the digital reward tool might, however, be subject to review if other means of rewarding and punishing users that bear an increased risk of discrimination are developed and integrated into the MTM system.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 953618. This document reflects only the author's view and the Agency is not responsible for any use that may be made of the information it contains.

4 Social dimension of Orchestra

According to the ORCHESTRA Grant Agreement, traffic management within the MTME will aim for transport and traffic that are optimal to the society, which will be supported by the enabling tools, guidelines, and models.[97] The latter, however, might not only benefit society by optimizing traffic management, but could potentially have detrimental societal effects that will be analysed in the following paragraphs.

4.1 Risk of Use of AI for employment and wages

For the development of an MTME in the ORCHESTRA project, Artificial intelligence (AI) approaches may be employed. This raises questions regarding ethical issues arising from the implementation of AI, notably its potential impact on the labour market.

While the use of AI will undoubtedly affect every sector of the economy and fundamentally reshape the work environment, promising greater productivity and efficiency as well as lower costs, concerns of job loss (even mass unemployment) and wage decline have accrued. In a similar vein, some experts fear that the automation of routine and low- to high-skilled tasks may increase economic and social inequality ("erosion of the middle class").[98] Discrimination could arise from different effects of emerging technologies on younger demographics which will have to develop new skill profiles to respond to new demands. Women, minorities, and poor people already suffering high levels of unemployment may also be disproportionally affected since they work in sectors prone to disruption.[99]

Fears of the displacement of jobs by technology are not a new phenomenon. They can be traced back for centuries.[100] Although they have regularly grown to be true regarding job losses in the short term, empirical evidence shows that in the long term automation has often led to the creation of jobs.[101] With regards to AI, its impact on the labour market is hard to quantify and substantial disagreement exists between economists, with a fifty-fifty divide between those that believe that robots and digital agents will displace significant numbers of workers and those that oppose that idea.[102] What is clear is that some sectors will be affected more gravely than others. Notably, high-

[97] See, for instance, ORCHESTRA Grant Agreement 953618, Part B, p. 25.

[98] European Parliament Research Service, "The ethics of artificial intelligence: Issues and initiatives", March 2020, available at: EPRS_STU(2020)634452_EN.pdf (europa.eu), p. 6; Lane/Saint-Martin, "The impact of Artificial Intelligence on the labour market: What do we know so far?", OECD Social, Employment and Migration Working Papers No. 256, p. 9f.

[99] European Parliament Research Service, "The ethics of artificial intelligence: Issues and initiatives", March 2020, available at: EPRS_STU(2020)634452_EN.pdf (europa.eu), p. 7

[100] ibid., p. 6.

[101] European Parliament Research Service, "The ethics of artificial intelligence: Issues and initiatives", March 2020, available at: EPRS_STU(2020)634452_EN.pdf (europa.eu) m. Verweis auf (Autor, 2015); Lane/Saint-Martin, "The impact of Artificial Intelligence on the labour market: What do we know so far?", OECD Social, Employment and Migration Working Papers No. 256, p. 30.

[102] European Parliament Research Service, "The ethics of artificial intelligence: Issues and initiatives", March 2020, available at: EPRS_STU(2020)634452_EN.pdf (europa.eu), p. 6; opinions of employers are equally divided, see Lane/Saint-Martin, "The impact of Artificial Intelligence on the labour market: What do we know so far?", OECD Social, Employment and Migration Working Papers No. 256, p. 34.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 953618. This document reflects only the author's view and the Agency is not responsible for any use that may be made of the information it contains.

skilled occupations involving non-routine cognitive tasks will presumably also be seriously exposed to AI.[103] Overall, there are many indications that AI will call for a reorganisation of tasks and re- or up-skilling workers within occupations.[104]

In the context of ORCHESTRA, too, there is the potential for individual tasks that previously required human intervention to be replaced by AI (i.e., air traffic controllers' tasks could be largely automated). The ethical implications associated with this shall be duly acknowledged in the project work.

4.2 Risk of excluding transport solutions – vulnerable road users

Even though all road users risk being injured in a road traffic accident, some individuals face a higher risk of accidents. The latter are commonly referred to as vulnerable road users. According to the classification put forward by the European Commission's VRUITS project[105], vulnerable road users are identified by the amount of external protection, task competency, and resilience and encompass, for instance, pedestrians, cyclists, and motorcyclists.[106] Children and the elderly are considered to be particularly vulnerable.[107]

While modern Intelligent Transport Systems (ITS) generally provide for active safety systems, mobility and comfort management, they often failed to adequately take the interests of vulnerable road users into account. Consequently, the VRUITS project sought to further improve road safety and comfort by integrating vulnerable road users as parts of ITS applications. During the course of the project, various ITS that aimed at enhancing the safety, mobility and comfort of vulnerable road users were tested, with ten of them providing significant benefits.[108] However, research suggests that ITS applications yield the potential for even more safe and comfortable transport for vulnerable road users.[109] In the course of the ORCHESTRA project, particular attention should be paid to the needs of vulnerable road users within the MTM ecosystem, while research on safe and comfortable intelligent traffic management should be closely followed accordingly.

[103] Lane/Saint-Martin, "The impact of Artificial Intelligence on the labour market: What do we know so far?", OECD Social, Employment and Migration Working Papers No. 256, p. 19, 22ff.
[104] ibid., p. 35.
[105] See https://cordis.europa.eu/project/id/321586/de.
[106] See Kerry Malone, Anne Silla, Charlotta Johanssen, Daniel Bell, Safety, mobility and comfort assessment methodologies of intelligent transport systems for vulnerable road users (Eur. Transp. Res. Rev. 2017 9:21), available at https://link.springer.com/content/pdf/10.1007/s12544-017-0235-y.pdf, p. 2.
[107] ibid., p. 3.
[108] See for the results in short https://cordis.europa.eu/article/id/198035-moving-in-the-right-direction-for-the-protection-of-vulnerable-road-users.
[109] See, for instance, Kerry Malone, Anne Silla, Charlotta Johanssen, Daniel Bell, Safety, mobility and comfort assessment methodologies of intelligent transport systems for vulnerable road users (Eur. Transp. Res. Rev. 2017 9:21), available at https://link.springer.com/content/pdf/10.1007/s12544-017-0235-y.pdf.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 953618. This document reflects only the author's view and the Agency is not responsible for any use that may be made of the information it contains.

4.3 Gender dimension

Gender is defined as the "social construction of women and men, of femininity and masculinity, which varies in time and place, and between cultures."[110] Moreover, gender "departs from the notion of sex to signal that biology or anatomy is not a destiny."[111] While applying a gender-sensitive lens, aspects on gender are taking into account in the whole research cycle. This leads to outcomes of gender-sensitive research.[112]

The concept of a gender dimension explain that gender itself is used as a analytical and explanatory variable in the research process.[113] Therefore, both the participation of women needs to be encouraged, as well as gender-specific research needs to be included.[114]

Taking this into account, the gender dimensions include aspects on gender inclusion in research teams, gender aspects of MTMEs themselves, as well as gender in relation to research participants in the living labs and the CoP.

4.3.1 Gender in Research Teams

The problem of possible gender inequality within the ambit of ORCHESTRA is not confined to the under-representation of women in transport but extends to the research conducted for the realisation of the project.

In 2009, women in research accounted for only 33 % of researchers in the EU, while the number of female PhD graduates equalled or outnumbered men in all fields of study except for, for instance, science, mathematics, computing and engineering.[115] Similarly, in 2018, women were close to reaching gender parity among doctoral graduates, but were still under-represented in technical professions in the fields of science, engineering and information and communication technologies, at the highest level in academia, among investors and also less likely to receive funding for their research.[116] Consequently, the under-representation of women in research is still relevant today and, thus, for the ORCHESTRA research project.

Various studies on the reasons and mechanisms that influence gender equality in EU research have been conducted throughout the years. According to the European Institute for Gender Equality, there are a number of persistent gender inequalities that result in the under-representation of women in research. A first major cause is gender segregation in research, mainly science, which is itself the result of gender stereotypes, gender division of labour and time constraints as well as covert barriers in organisational structures.[117] Moreover, women scientists still face many career challenges and are

[110] European Commission, Research & Innovation, Toolkit Gender in EU-funded research, 2014, available at: https://op.europa.eu/de/publication-detail/-/publication/c17a4eba-49ab-40f1-bb7b-bb6faaf8dec8.
[111] ibid.
[112] ibid.
[113] ibid.
[114] ibid.
[115] European Commission, She Figures 2012 [2012], available at https://op.europa.eu/en/publication-detail/-/publication/ba8dc59b-61b8-4c03-9176-373fd9ddac82/language-en, p. 5.
[116] European Commission, She Figures 2021 [2021], available at https://op.europa.eu/en/web/eu-law-and-publications/publication-detail/-/publication/61564e1f-d55e-11eb-895a-01aa75ed71a1.
[117] European Institute for Gender Equality, Gender in research [2016], available at https://eige.europa.eu/publications/gender-research, p. 4.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 953618. This document reflects only the author's view and the Agency is not responsible for any use that may be made of the information it contains.

thus under-represented in leadership positions, particularly among academic gatekeepers and research organisations.[118] This might also be one reason why there is still a significant gender bias in access to research funding.[119] Lastly, gender-blind and gender-biased research, organisational culture and institutional process fail to recognize and address gender differences.[120]

On an EU level, in 1999, the European Commission recognised the under-representation of women in research and stressed the importance of developing a coherent approach towards promoting women in research with the aim of achieving at least a 40 % representation for women in that field of EU research[121], an objective which was reiterated shortly after by the Council of the European Union in its resolution on women and science.[122] The following years saw several efforts by the European Commission to promote gender equality.[123] In particular, in 2000, it adopted a Communication that sought to establish a European research area and particularly highlighted the importance of more prominence to the place and role of women in research.[124] In 2008, the European Parliament likewise adopted a resolution on women and science.[125] Most importantly, it recognised the reasons and mechanisms hindering gender equality in science and called on all EU institutions to change that situation. Finally, the EU's Horizon 2020 framework considers the promotion of gender equality in science and innovation a specific commitment of the Union.[126]

In its 2011 Toolkit Gender in EU-funded research, the European Commission stated that gender in research required actions relating to both the participation of women in research and to the gender dimension of research, i.e., that gender is considered as a crucial analytical and explanatory variable in research.[127] To this end, it provided for suggestions to make research gender-sensitive. In particular, gender should be taken into account at all stages of the research cycle.[128] Moreover, selection and recruitment should avoid gender biases by ensuring open and impartial selection procedures and using explicit and transparent selection criteria, creating adequate working

[118] European Institute for Gender Equality, Gender in research [2016], available at https://eige.europa.eu/publications/gender-research, p. 4 – 6.
[119] ibid., p. 6.
[120] ibid., p. 7.

[121] European Commission, Communication from the Commission – "Women and science" – Mobilising women to enrich European research [1999] COM(1999) 76 final, p. 4.
[122] Council of the European Union, Council Resolution of 20 May 1999 on women and science [1999] OJ C 201/1.
[123] See on this development European Institute for Gender Equality, Gender in research [2016], available at https://eige.europa.eu/publications/gender-research, p. 8.

[124] European Commission, Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions - Towards a European research area [2000] COM/2000/0006 final, 5.3.

[125] European Parliament, Resolution of 21 May 2008 on women and science (2007/2206(INI)) [2008] OJ C 279E/40.

[126] 2013/743/EU: Council Decision of 3 December 2013 establishing the specific programme implementing Horizon 2020 - the Framework Programme for Research and Innovation (2014-2020) and repealing Decisions 2006/971/EC, 2006/972/EC, 2006/973/EC, 2006/974/EC and 2006/975/EC [2013] OJ L 347/965.
[127] European Commission, Toolkit Gender in EU-funded research [2011], available at https://op.europa.eu/de/publication-detail/-/publication/c17a4eba-49ab-40f1-bb7b-bb6faaf8dec8, p. 10.
[128] ibid., p. 13.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 953618. This document reflects only the author's view and the Agency is not responsible for any use that may be made of the information it contains.

conditions and culture, and setting up monitoring systems.[129] Lastly, gender should play a role in research content as well, ranging from research ideas and hypotheses to project design and research implementation and finally to the dissemination phase.[130] When conducting research for ORCHESTRA, this toolkit should be kept in mind as a starting point for gender equality in the research project.

4.3.2 Gender and MTMEs

Transport projects like ORCHESTRA and policies aim at equally benefitting everyone in the same way. However, professional literature suggests that transport is not gender neutral. There are significant differences in travel patterns of men and women which are tied to the societal roles prescribed to men and women. For instance, women, in their role as caregivers or taking up multiple roles at a time (being responsible for care as well as income activities), tend to use different modes of transport in more complex ways than men.[131] They often make more chained shorter trips, closer to home, and with multiple stops. They pay more attention to sustainable transport means and use public transport at different times (e.g., less at night). Women are also generally less likely to own a car and cease driving earlier and are thus more dependent on non-motorised transport.[132]

At the same time, transport infrastructure and services fail to take these differences into account. Employment-related mobility which benefits peak-hour male commuter patterns and the needs of car users going into city centres has led to a bias towards the travel needs of men despite women being the main users of public transport. Moreover, the quality and safety of public transport means differs for women and men since women are more exposed to gender-based violence than men. Reduced access to transportation also affects access to labour markets, professional development, economic status, and personal well-being.[133] Gender inequalities are also persistent in the transport labour market where men usually take up the jobs as drivers, technicians or occupations involving physical work, while women predominate in service-related or administrative jobs.[134]

Consequently, gender-awareness must be created, shifting the employment-related concept of mobility towards a mobility concept which accounts for all travel associated with care and home tasks (termed a “mobility of care” by Sánchez de Madariaga). This involves gathering more information on gender in transport, notably by using sex-disaggregated travel data.[135] Care trips must be adequately accounted for in these datasets and their significance visually represented

---

[129] European Commission, Toolkit Gender in EU-funded research [2011], available at https://op.europa.eu/de/publication-detail/-/publication/c17a4eba-49ab-40f1-bb7b-bb6faaf8dec8, p. 14.

[130] ibid., p. 15.

[131] EIGE, “Gender in transport”, 2016, available at: https://eige.europa.eu/gender-mainstreaming/policy-areas/transport p. 3; Sánchez de Madariaga, “From women in transport to gender in transport”, Journal of International Affairs, Vol. 67/1, p. 48.

[132] EIGE, “Gender in transport”, 2016, available at: https://eige.europa.eu/gender-mainstreaming/policy-areas/transport , accessed 11.10.2021, p. 3.

[133] Sánchez de Madariaga, “From women in transport to gender in transport”, Journal of International Affairs, Vol. 67/1, p. 49.

[134] EIGE, “Gender in transport”, 2016, available at: https://eige.europa.eu/gender-mainstreaming/policy-areas/transport , accessed 11.10.2021, p. 6.

[135] ibid., 9.

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 953618. This document reflects only the author’s view and the Agency is not responsible for any use that may be made of the information it contains.

accordingly.[136] Gender budgeting can make visible how much money is spent for women and men respectively, and monitoring and evaluation mechanisms can contribute to the efficient implementation of gender objectives.[137] Women, who usually are less involved in decision-making processes in the transport sector, shall participate equally.[138] In this way, gender objectives should also play a significant role in ORCHESTRA. Since women, in their role as care-givers, often use multimodal transport and suffer from more time poverty because of their numerous and various daily tasks, they could benefit from the development of a MTME and the associated efficiency gains. With men taking on an increasing proportion of care tasks, the question of a mobility of care will become more and more significant for both sexes.

4.3.3 Gender relation of research participants in living labs and CoP

The misrepresentation of female experts in the transport sector and its potential consequences with regard to policy making is an issue.

Therefore, the ORCHESTRA consortium should implement measures, in order to foster the gender balance concerning the research participants in living labs and the CoP. In order to create a dialogue on the topic, that includes all project partners, the relevance of the issue was explained to the consortium in M4.

Since the misrepresentation of female actors in the transport sector is likely to result in transport policies and decisions that intensify gender inequalities, actors involved in the ORCHESTRA project need to pay close attention to the relevance of gender when carrying out their tasks. To this end, gender aspects must already be taken into account when establishing the CoP since the CoP members' feedback will eventually influence other research tasks and, thus, the ORCHESTRA research findings as a whole. Consequently, a gender balance should be achieved in the CoP with female and male experts ideally making up 50 % of the participants each.

In order to reach that goal, the following questions were addressed to the consortium:

- Does your organisation have a gender equality policy or other means to tackle the aforementioned gender inequality issues? If so, how do these look like?
- How can we make sure that female experts are sufficiently involved in the CoP? Ideally, how can we reach a gender balance in the CoP?

Feedback from the consortium and assessment/ policy

[136] Sánchez de Madariaga, "From women in transport to gender in transport", Journal of International Affairs, Vol. 67/1, p. 58ff.
[137] EIGE, "Gender in transport", 2016, available at: https://eige.europa.eu/gender-mainstreaming/policy-areas/transport, p. 13.
[138] For instance, according to a recent EU study on women employment in the urban public transport sector, women represent roughly 20 % of the management boards (source: Project WISE, Project Report - Women Employment in Urban Public Transport Sector [2018], available at https://www.etf-europe.org/wp-content/uploads/2018/09/WISE-I-Report_EN.pdf, p. 5); EIGE, "Gender in transport", 2016, available at: https://eige.europa.eu/gender-mainstreaming/policy-areas/transport , p. 6.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 953618. This document reflects only the author's view and the Agency is not responsible for any use that may be made of the information it contains.

After careful consideration of the feedback provided by project partners regarding a potential gender equality policy for CoP members, the main strategies in the field of gender equality deployed by the stakeholders and their suggestions for gender equality in the CoP can be summarised as follows:

Most stakeholders seek to achieve diversity within their institution at an early stage in the hiring process in order to make sure that men and women (and other minority groups) are represented equally. While some rely on informal policies or general guidelines in that regard, others have drafted written policies specifically for the purpose of gender equality. This is usually accompanied by targeted initiatives, courses and workshops that support and promote women. For the purpose of maintaining gender equality, some stakeholders have opted for the creation of internal supervision bodies such as diversity offices.

Based on their own experiences, many stakeholders have suggested to increase the number of female CoP participants by either directly contacting female representatives of a company or suggesting to those companies that female representatives are particularly welcome. Moreover, where more than one representative is proposed by the company to hold an interview, their gender could be registered, and the representative could be selected based on that factor to achieve an equal gender balance. Alternatively, the interview process could be extended to encompass several rounds with both the male and the female representatives. If there are more male than female CoP members, stakeholders have proposed that the male representatives could be encouraged to provide "multigender answers". Moreover, each CoP could have two main contacts, one male and one female one. Lastly, stakeholders have highlighted the importance of achieving a good gender balance also with regard to the persons preparing and performing the interviews and workshops.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 953618. This document reflects only the author's view and the Agency is not responsible for any use that may be made of the information it contains.

5 Ethical issues from CoP involvement

Ethical issues may also arise out of the involvement of CoP in the process of stakeholder exchange. The CoP will be established in the beginning of the project and may be extended during the project, in order to take into account the view of practitioners in the traffic and transport sector through workshops and interviews. Thus, the relevance of the research results gained in ORCHESTRA will be validated.[139]

Special attention needs to be given to data protection requirements, as well as the protection of trade secrets of CoP members.

5.1 Personal data protection requirements

The necessary data protection requirements derive out of the General Data Protection Regulation.

In order to brief the consortium on the topic of personal data protection a workshop on ethics requirements was hosted by IKEM at M2 of the project. The workshop covered an introduction to ethics in research and provided an overview of the data flows in the project. Furthermore, it introduced GDPR requirements and presented templates on informed consent.

Moreover, relevant information concerning personal data protection requirements are included in D8.2 POPD-Requirement No.2. Furthermore, the applicability of the GDPR, as well as adequate levels of protection for non-applicability for project partners from non-European countries is analysed in D8.3- NEC-Requirement No.3.

5.2 Protection of trade secrets

Through the communicative involvement of the CoP and the data collection through workshop and interviews, business secrets might be shared by CoP members.

In order to handle the shared business secrets in accordance with European law the legal requirements on the protection of business secrets need to be analysed. The following information on the protection of trade secrets has been shared with the consortium prior to the submission of this report during the executive board meeting in M4.

5.2.1 Overview of legal framework

On an EU level, the primary source of protection of trade secrets is EU Directive 2016/943 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure.[140] According to its Article 2 section 1, ‘trade secret’ means any information that is secret in the sense that it is not generally known among or readily accessible to persons within the circles that normally deal with that kind of information, that has commercial value because it is secret, and that has been subject to reasonable steps to keep it secret. In the course of conducting the interviews with CoP members, the latter might disclose information that

[139] GA Orchestra, Part B, p. 10.

[140] Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure (Text with EEA relevance), OJ L 157, 15.6.2016, p. 1–18.

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 953618. This document reflects only the author’s view and the Agency is not responsible for any use that may be made of the information it contains.

falls within the ambit of the aforementioned definition. In particular, CoP members might elaborate on the technical requirements for the multimodal traffic management ecosystem and thereby reveal technical know-how that is exclusively known to their company and generally prevented from being disclosed, thereby generating competitive advantages.

According to Article 3 section 1 letter d of the Directive, the acquisition of a trade secret is considered lawful when it is obtained by a practice which, under the circumstances, is in conformity with honest commercial practices. On the contrary, Article 4 section 2 letter b of the Directive deems the acquisition of a trade secret without the consent of the trade secret holder to be unlawful, if it is carried out by conduct which, under the circumstances, is considered contrary to honest commercial practices. The latter term is not defined in the Directive itself, however, guidance can be drawn from TRIPS agreement.[141] Article 39 section 2 of the TRIPS agreement covers the protection of 'undisclosed information' and yields a definition of this term that is similar to the one given by Article 2 section 1 of the Directive.[142] Moreover, Article 39 section 2 of the TRIPS agreement likewise prohibits the disclosure, acquisition or usage of undisclosed information contrary to honest commercial practices. The latter is defined in footnote 10 of the TRIPS agreement as breach of contract, breach of confidence and inducement to breach, which includes the acquisition of undisclosed information by third parties who knew or were grossly negligent in failing to know, that such practices were involved in the acquisition. The voluntary disclosure of trade secrets by CoP members does not amount to a breach of contract or confidence since interviewers are not aware of the secret nature of the information shared with them during the interviews. While the questions interviewers will ask CoP members might be classified as an 'inducement to breach', the latter requires at least gross negligence on behalf of the interviewers or researchers who subsequently use the information to develop the MTME. However, interviewers and researchers will assume that the interview partners will follow their company's trade secret policy and thus act in good faith when conducting the interview. Nevertheless, in order to rule out doubts on behalf of the interviewers and researchers as regards potential trade secrets, the interview partners should be informed about the nature of and law on trade secrets and reminded to not disclose their company's trade secrets unless instructed to do so.

Moreover, the use or disclosure of a trade secret is unlawful pursuant to Article 4 section 3 letter b of the Directive, if the person the trade secret has been revealed to is in breach of a confidentiality agreement or any other duty not to disclose the trade secret. If the interview participants consider any information they have given to be a trade secret after the interview has been conducted, it will be possible to sign a non-disclosure agreement with them. The latter prevents those trade secrets from being disclosed publicly in accordance with Article 4 section 3 letter b of the Directive.

In case of unlawful acquisition, use and disclosure of trade secrets, Articles 6 to 9 of the Directive oblige Member States to set out measures, procedures, and remedies to ensure civil redress against the infringing party. Moreover, Articles 10 to 14 prescribe the instalment of provisional and

[141] WTO, Agreement on trade-related aspects of intellectual property rights, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1C, 1869 U.N.T.S. 299, 33 I.L.M. 1197 (1994). For the EU accession see 94/800/EC: Council Decision (of 22 December 1994) concerning the conclusion on behalf of the European Community, as regards matters within its competence, of the agreements reached in the Uruguay Round multilateral negotiations (1986-1994), OJ L 336, 23.12.1994, p. 1–2.

[142] See on this CJEU, judgment of 5 February 2018, T-235/15 - Pari Pharma/EMA, ECLI:EU:T:2018:65, paras 112 – 114.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 953618. This document reflects only the author's view and the Agency is not responsible for any use that may be made of the information it contains.

precautionary measures in order to avoid the infringement of trade secrets as well as injunctions, corrective measures and damages to sanction any unlawful actions within the scope of the Directive.

With regard to organizations based in Norway, the EEA Joint Committee's Decision No 91/2019 of 29 March 2019[143] aimed at amending Annex XVII (Intellectual Property) to the EEA Agreement and incorporating EU Directive 2016/943 into the latter. The Decision was supposed to enter into force on 30 March 2019 provided that all the notifications under Article 103 section 1 of the EEA Agreement would have been made.[144] In Switzerland, however, EU Directive 2016/943 is not directly applicable. Instead, Switzerland is bound by Article 39 of the TRIPS agreement[145] and several scattered national laws such as criminal laws[146], the Swiss Code of Obligations[147] and the Law Against Unfair Competition[148].

5.2.2 Advise for consortium and CoP members

Prior to conducting the interview, CoP members need information, that any ORCHESTRA research findings and, consequently, information CoP members reveal during the course of their interview, might eventually be published. In order to remind them of their obligation to not disclose information that amount to trade secrets within the meaning of EU Directive 2016/943, or other security and safety relevant information, CoP members will receive an information sheet that briefly sets out the legal framework and reminds participants to safeguard their company's trade secrets. The latter could read as follows:

Information on Trade Secrets and other security and safety relevant information

In order to prevent your company's trade secrets from being exploited, we kindly ask you to carefully read the following information on trade secrets.

EU Directive 2016/943 (hereinafter 'the Directive') prohibits the unlawful acquisition, use and disclosure of trade secrets. The latter is defined as information that is secret in the sense that it is not generally known among or readily accessible to persons within the circles that normally deal with that kind of information, that has commercial value because it is secret, and that has been subject to reasonable steps to keep it secret. However, as long as the acquisition and use of trade secrets is in conformity with honest commercial practices, it is lawful under the Directive. This particularly means that the party which receives information classified as trade secrets within the meaning of the Directive must act in good faith when acquiring or disclosing them in order to avoid legal action against it.

---

[143] Decision of the EEA Joint Committee No 91/2019 of 29 March 2019 amending Annex XVII (Intellectual Property) to the EEA Agreement [2020/839], OJ L 210, 2.7.2020, p. 76–77.

[144] EEA Joint Committee Decision No 91/2019, Article 3.

[145] See, for instance, https://www.wto.org/english/tratop_e/trips_e/amendment_e.htm.

[146] See, for instance, Swiss Criminal Code (Strafgesetzbuch) of 21 December 1937, AS 54 757, Article 162 (on infringement of fabrication or trade secret).

[147] See, for instance, Swiss Civil Code (Zivilgesetzbuch) of 10 December 1907, AS 24 233, Part 5 on the Law of Obligations, Article 321a on the employee's duty of loyalty.

[148] Swiss Law Against Unfair Competition (Bundesgesetz über Kartelle und andere Wettbewerbsbeschränkungen) of 1 February 1996, AS 1996 546.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 953618. This document reflects only the author's view and the Agency is not responsible for any use that may be made of the information it contains.

Research findings generated during the course of the ORCHESTRA project may eventually be made publicly available through reports. Hence, information you share during the course of your interview will not only influence research activities conducted on the basis of your interview, but will also be included in reports and analysis that will be published online. In order to safeguard your company's trade secrets and adhere to the protection standard enshrined in the Directive as well as the applicable national laws, please consider in advance which information you are authorised to disclose according to your company's trade secret policy. It is generally assumed that any information you share during the interview does not amount to a trade secret within the meaning of the Directive.

In any case, after your interview has been conducted, we will share the interview record with you in order to provide you with the opportunity to review your answers. If you consider any information revealed to us during the course of the interview to be a trade secret that you have disclosed unintentionally, you may adapt the information in question.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 953618. This document reflects only the author's view and the Agency is not responsible for any use that may be made of the information it contains.

6 Conclusions

The findings of the deliverable contribute to the implementation of ethical and secure concepts for MTMEs. The development of ethical and secure concepts foster the trust in automated systems, which will have a positive effect on the acceptance of MTMEs by society.

The findings are relevant with respect to the following objectives of the ORCHESTRA project:

- *O1: Establish a common understanding of multimodal traffic management (MTM) concepts and solutions.* The work in WP2 on target vision, scenarios and White paper must take the social dimension and the ethical issues of digitalization and CoP involvement into account.
- *O2: Define MTME where traffic managements in different modes and areas (rural and urban) are coordinated to contribute to a more balanced and resilient transport system, bridging current barriers and silos.* The work in WP3 on the polycentric and multimodal traffic management architecture must take social dimension and the ethical issues of digitalization into account.
- *O3: Support MTME realisation and deployments.* The work in WP4 on tools, models and guidelines must take the ethical issues of digitalization and the social dimension into account.
- *O4: Validate and calibrate MTME with respect to organisational issues, functionality, capability and usability.* The living labs in WP5 and on the work on evaluations and lessons learned in WP6 must take the ethical issues of digitalization, the social dimension, and the ethical issues of CoP involvement into account.

The issue of security requirements for MTMEs will be further developed in T2.2 Environment analysis, where the European legal framework on cybersecurity will be analysed more detailed. The implementation of a secure concept for MTME is necessary in order for relevant stakeholders to be willing to participate. Therefore, the digital infrastructure needs to apply cybersecurity requirements deriving out of regulation. Moreover, the findings on the topic of trust in autonomous technologies are important for T2.1 Target visions, as well as for the topic of acceptance, which will be elaborated during T2.2 Environment analysis.

However, the analysis of the social dimension of MTMEs shows that, the both the risk of use of AI for employment and wages, as well as for excluding transport solutions need to be taken into account. Nevertheless, direct answers to the wider societal challenges of the effect on AI on the labour market cannot derive out of ORCHESTRA. Moreover, the report shows, that special care needs to be given to the topic of gender. This needs to be considered both internally within research teams, as well as throughout the involvement of the CoP. The deriving gender-sensitive research may fill existing research gaps.

Furthermore, the ethical issues concerning data protection and the protection of trade secrets can be dealt with in ethical compliance, by following the suggested management approach. Whenever, personal data from CoP members is proceeded during the tasks, which include stakeholder involvement, GDPR requirements need to be applied.

The report shows, that the implementation of an ethical and secure concept of is possible, as long as specific regulation and social dimensions are taking into account during all stages of the research cycle.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 953618. This document reflects only the author's view and the Agency is not responsible for any use that may be made of the information it contains.

7 References

7.1 Primary Sources

Case law

Paris Pharma v EMA (T-235/15) [2018], CJEU, ECLI:EU:T:2018:65.

International law

Convention for the Protection of Human Rights and Fundamental Freedoms [1950] ETS 5.

UN General Assembly, Universal Declaration of Human Rights, 10 December 1948, 217 A (III).

WTO Agreement: Marrakesh Agreement Establishing the World Trade Organization, Apr. 15, 1994, 1867 U.N.T.S. 154, 33 I.L.M. 1144 (1994).

EU Legislation

Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products [1985] OJ L 210/29.

Directive (EU) 2009/12/EC of the European Parliament and of the Council of 11 March 2009 on airport charges [2009] OJ L 70/11.

Directive (EU) 2010/40/EU of the European Parliament and of the Council of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport [2010] OJ L 207/1.

Directive (EU) 2012/34/EU of the European Parliament and of the Council of 21 November 2012 establishing a single European railway area [2012] OJ L 343/32.

Directive (EU) 2015/1535 of the European Parliament and of the council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services [2015] OJ L 241/1.

Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure (Text with EEA relevance), OJ L 157.

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union [2016] OJ L 194/1.

Regulation (EC) No 549/2004 of the European Parliament and of the Council of 10 March 2004 laying down the framework for the creation of the single European sky [2004] OJ L 96/1.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 953618. This document reflects only the author's view and the Agency is not responsible for any use that may be made of the information it contains.

Regulation (EU) 1291/2013 of the European Parliament and of the Council of 11 December 2013 establishing Horizon 2020 – the Framework Programme for Research and Innovation [2013] OJ L 347/104.

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 [2016] OJ L 119/1.

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 [2019] OJ L 151/15.

National Legislation

German Basic Law (*Bürgerliches Gesetzbuch*) of 1 January 1900, BGBl. I p. 42.

German General Equal Treatment Act (*Allgemeines Gleichbehandlungsgesetz*) of 18 August 2006, BGBl. I p. 1897, 1910.

German Road Traffic Act (*Straßenverkehrsgesetz)* of 1 June 1909, BGBl. I p. 310.

Swiss Civil Code (*Zivilgesetzbuch*) of 10 December 1907, AS 24 233.

Swiss Criminal Code (*Strafgesetzbuch*) of 21 December 1937, AS 54 757.

Swiss Law Against Unfair Competition (*Bundesgesetz über Kartelle und andere Wettbewerbsbeschränkungen*) of 1 February 1996, AS 1996 546.

7.2 Secondary Sources

European Commission Documents

Commission, "Adapting liability rules to the digital age and circular economy" [2021] Ares. (2021)4266516 - 30/06/2021.

Commission, "Algorithmic discrimination in Europe - Challenges and opportunities for gender equality and non-discrimination law".

Commission, "Communication from the Commission - Coordinated Plan on Artificial Intelligence" [2018] COM/2018/795 final.

Commission, "Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions - Towards a European research area" [2000] COM/2000/0006 final.

Commission, "Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions: Fostering a

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 953618. This document reflects only the author's view and the Agency is not responsible for any use that may be made of the information it contains.

European approach to Artificial Intelligence, Annex: Coordinated Plan on Artificial Intelligence 2021 Review" [2021] COM (2021) 205 final.

Commission, "Ethics of Connected and Automated Vehicles - Recommendations on road safety, privacy, fairness, explainability and responsibility" [2020].

Commission, "Joint Communication to the European Parliament and the Council - The EU's Cybersecurity Strategy for the Digital Decade" JOIN/2020/18 final.

Commission, "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.

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" [2021] COM/2021/206 final.

Commission, "She Figures 2012. Gender in Research and Innovation" [2012].

Commission, "White Paper on Artificial Intelligence - A European approach to excellence and trust" [2020] COM (2020) 65 final.

Commission, "White Paper on Transport" COM/2011/0144 final.

Commission, "Women and science. Mobilising women to enrich European research" [1999] COM (1999) 76 final.

Commission, Research & Innovation, "Toolkit Gender in EU-funded research" [2011].

Council of the EU

Council of the EU, "Presidency conclusions - The Charter of Fundamental Rights in the context of Artificial Intelligence and Digital Change" [2020] 11481/20.

Council of the EU, "Council Decision of 22 December 1994 concerning the conclusion on behalf of the European Community, as regards matters within its competence, of the agreements reached in the Uruguay Round multilateral negotiations (1986-1994)", 94/800/EC, OJ L 33.

Council of the EU, "Council Resolution of 20 May 1999 on women and science" [1999] OJ C 201/1.

Council of the EU, "Council Decision of 3 December 2013 establishing the specific programme implementing Horizon 2020 - the Framework Programme for Research and Innovation (2014-2020) and repealing Decisions 2006/971/EC, 2006/972/EC, 2006/973/EC, 2006/974/EC and 2006/975/EC" [2013] 2013/743/EU, OJ L 347/965.

European Parliament Resolutions

European Parliament, "Resolution of 20 October 2020 with Recommendations to the Commission on a Civil Liability Regime for Artificial Intelligence" [2020] 2020/2014/INL.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 953618. This document reflects only the author's view and the Agency is not responsible for any use that may be made of the information it contains.

European Parliament, "Resolution of 21 May 2008 on women and science" [2008] 2007/2206/INI, OJ C 279E/40.

European Parliament, "Resolution with recommendations to the Commission on a framework of ethical aspects of artificial intelligence, robotics and related technologies" [2020] 2020/2012/INL.

Books

Paal/Pauly, "Datenschutz-Grundverordnung Bundesdatenschutzgesetz" (3rd edition), 2021.

Articles

Eidenmüller, "The Rise of Robots and the Law of Humans", ZEuP 2017, 765.

Herbert Zech, "Liability for AI: Public Policy Considerations", ERA Forum 2021, 22:147.

Malone/Silla/Johanssen/Bell, "Safety, mobility and comfort assessment methodologies of intelligent transport systems for vulnerable road users", Eur. Transp. Res. Rev. 2017 9:21.

Raars/Fors/Pink, "Trusting autonomous vehicles: An interdisciplinary approach", Transportation Research Interdisciplinary Perspectives, Volume 7, 2020.

Sánchez de Madariaga, "From women in transport to gender in transport", Journal of International Affairs, Vol. 67/1.

Others

Bird/Fox-Skelly/Jenner/Larbey/Weitkamp/Winfield, European Parliament Research Service, "The ethics of artificial intelligence: Issues and initiatives", PR 634.452, March 2020.

CORDIS Fact Sheet, "Improving the Safety and Mobility of Vulnerable Road Users through its Applications", available at: https://cordis.europa.eu/project/id/321586/en.

CORDIS Results in Brief, "Improving the Safety and Mobility of Vulnerable Road Users through its Applications", available at: https://cordis.europa.eu/article/id/198035-moving-in-the-right-direction-for-the-protection-of-vulnerable-road-users.

Council of Europe, Committee on Legal Affairs and Human Rights, "Report on legal aspects of "autonomous" vehicles", AS Jur (2020) 20.

Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques, 0829/14/EN WP216.

Decision of the EEA Joint Committee No 91/2019 of 29 March 2019 amending Annex XVII (Intellectual Property) to the EEA Agreement [2020/839], OJ L 210.

ENISA, "Cybersecurity Certification: Candidate EUCC Scheme V1.1.1", 2021.

European Data Protection Board, "Guidelines 07/2020 on the concepts of controller and processor in the GDPR", 2020.

European Institute for Gender Equality, "Gender in research", 2016.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 953618. This document reflects only the author's view and the Agency is not responsible for any use that may be made of the information it contains.

Lane/Saint-Martin, “The impact of Artificial Intelligence on the labour market: What do we know so far?”, OECD Social, Employment and Migration Working Papers No. 256.

Orwat, “Risks of Discrimination through the Use of Algorithms”, German Federal Anti-Discrimination Agency.

SAE International, “Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles”, 2021, J3016_202104.

Senior Officials Group Information Systems Security (SOG-IS), “Mutual Recognition Agreement of Information Technology Security Certificates”, 2010.

The WISE Project, “Project Report - Women Employment in Urban Public Transport Sector”, 2018.

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 953618. This document reflects only the author’s view and the Agency is not responsible for any use that may be made of the information it contains.

Members of the ORCHESTRA consortium

ITS Norway	**ITS Norway** c/o Tekna – Teknisk-naturvitenskapelig forening Postboks 2312 Solli NO-0201 Oslo Norway its-norway.no	**Project Coordinator:** Runar Søråsen runar.sorasen@its-norway.no **Dissemination Manager:** Jenny Simonsen jenny.simonsen@its-norway.no
SINTEF	**SINTEF AS** NO-7465 Trondheim Norway www.sintef.com	**Technical Manager:** Marit Natvig Marit.K.Natvig@sintef.no
TU Delft	**Technische Universiteit Delft** Stevinweg 1 2628 CN Delft The Netherlands	**Evaluation Manager:** Alexei Sharpanskykh O.A.Sharpanskykh@tudelft.nl
ROSAS	**ROSAS Center Fribourg** Passage de Cardinal 13B Halle bleue CH-1700 Fribourg Switzerland info@rosas.center	**Contact:** Lucio Truaisch lucio.truaisch@rosas.center
CERTX	CERTX AG Route de l'Ancienne Papeterie 106 CH-1723 Marly Switzerland	**Contact:** Samuel Rieder samuel.rieder@certx.com
IKEM	**Institut Fur Klimaschutz Energie Und Mobilitat-Recht, Okonomie Und Politik Ev (IKEM)** Magazinstraße 15-16 10179 Berlin Germany	**Data Manager / Legal, Privacy and Policy Issues Officer (LEPPI) officer:** Anne Freiberger anne.freiberger@ikem.de
IOTA FOUNDATION	**IOTA Foundation** c/o Nextland Straßburger Straße 55 10405 Berlin Germany	**Contact:** Michele Nati michele@iota.org Siddhant Ghongadi siddhant.ghongadi@iota.org
SEA Milan Airports	**Societa Per Azioni Esercizi Aeroportuali Sea (SEA)** Presso Aeroporto Linate 20090 Segrate MI Italy	**Contact:** Massimo Corradi massimo.corradi@seamilano.eu

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 953618. This document reflects only the author's view and the Agency is not responsible for any use that may be made of the information it contains.

deepblue consulting & research	**Deep Blue Srl** Via Ennio Quirino Visconti, 8 00193 Roma Italy	**Innovation Manager:** Alessandra Tedeschi alessandra.tedeschi@dblue.it
RÉPUBLIQUE FRANÇAISE Cerema	**Cerema** 25 Avenue François Mitterrand 69500 Bron France	**Contact:** Sylvain Belloche Sylvain.Belloche@cerema.fr
TECHNOLOGY GRUPPO FERROVIE DELLO STATO ITALIANE	**FSTechnology SpA** Piazza della Croce Rossa, 1 00161 Roma RM Italy	**Contact:** Jessica Bonanno jessica.bonanno@it.ey.com
Information Sharing Company	**Information Sharing Company Srl (ISC)** Via di Tor Pagnotta, 94/95 00143 Roma Italy	**Contact:** Antonio Martino a.martino@gruppoisc.com
APPLIED AUTONOMY	**Applied Autonomy AS** Kirkegardsveien 45 NO-3601 Kongsberg Norway	**Contact:** Olav Madland olav.madland@appliedautonomy.no
HERØYA INDUSTRIPARK www.heroya-industripark.no	**Herøya Industripark AS** Hydrovegen 55 NO-3936 Porsgrunn Norway	**Contact:** Tone Rabe tone.rabe@hipark.no
enav	**ENAV SpA** Via Salaria, 716 00138 Roma Italy	**Contact:** Patrizia Criscuolo Patrizia.Criscuolo@technosky.it
Statens vegvesen Norwegian Public Roads Administration	**Statens vegvesen** Rynsengfaret 6A NO-0667 Oslo Norway	**Contact:** Elisabeth Skuggevik elisabeth.skuggevik@vegvesen.no

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 953618. This document reflects only the author's view and the Agency is not responsible for any use that may be made of the information it contains.