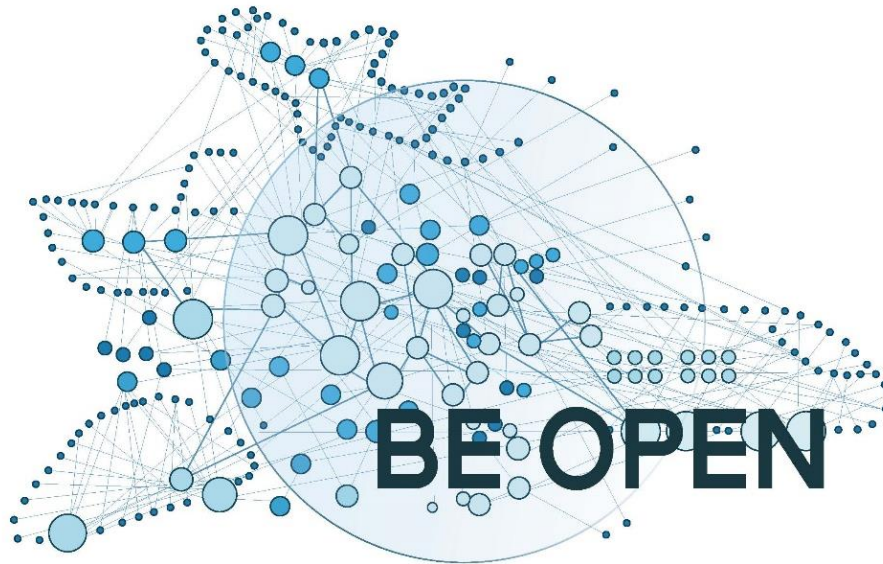




This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 824323

This document reflects only the views of the author(s). Neither the Innovation and Networks Executive Agency (INEA) nor the European Commission is in any way responsible for any use that may be made of the information it contains.



European forum and oBsErvatory for OPEN science in transport

Project Acronym: **BE OPEN**

Project Title: **European forum and oBsErvatory for OPEN science in transport**

Project Number: **824323**

Topic: **MG-4-2-2018 – Building Open Science platforms in transport research**

Type of Action: **Coordination and support action (CSA)**

Open Science in transport research: legal issues and fundamental principles

Final

Deliverable Title:	D 4.1 Open Science in transport research: legal issues and fundamental principles
Work Package:	WP4: Code of Conduct on Open Science in Transport
Due Date:	31/08/2020
Submission Date:	31/08/2020
Start Date of Project:	01/01/2019
Duration of Project:	30 Months
Organisation Responsible of Deliverable:	Osborne Clarke Rechtsanwälte Steuerberater Partnerschaft mbB (Osborne Clarke)
Version:	1.0
Status:	Final
Author name(s):	Dr. Marc Störing (Osborne Clarke), Christian von Bühler (Osborne Clarke)
Reviewer(s):	Kristel Palts (DLR), Dr. Adewole Adesiyun (FEHRL)
Nature:	<input checked="" type="checkbox"/> R – Report <input type="checkbox"/> P – Prototype <input type="checkbox"/> D – Demonstrator <input type="checkbox"/> O - Other
Dissemination level:	<input checked="" type="checkbox"/> PU - Public <input type="checkbox"/> CO - Confidential, only for members of the consortium (including the Commission) <input type="checkbox"/> RE - Restricted to a group specified by the consortium (including the Commission Services)

Document history			
Version	Date	Modified by (author/partner)	Comments
0.1	29/05/2020	Dr. Marc Störing, Christian von Bühler (Osborne Clarke)	Initial creation of document.
0.2	14/08/2020	Dr. Marc Störing, Christian von Bühler (Osborne Clarke)	Final draft for peer-review.
0.3	25/08/2020	Kristel Palts (DLR), Dr. Marc Störing, Christian von Bühler (Osborne Clarke)	Amendments following peer-review by DLR.
0.4	28/08/2020	Dr. Adewole Adesiyun (FEHRL)	Amendments following peer-review by FEHRL.
1.0	31/08/2020	Dr. Marc Störing, Christian von Bühler (Osborne Clarke)	Final version for submission.

Contents

List of Figures.....	5
List of Tables.....	5
Abbreviations and Terminology	6
Executive Summary	7
1 Introduction.....	9
1.1 Purpose of the Document	9
1.2 Methodology	11
2 Legal Issues and fundamental Principles.....	13
3 Legal Aspects	18
3.1 Legal Protection of Data (Intellectual Property Rights).....	19
3.1.1 Copyright	21
3.1.2 Trade Secrets	26
3.1.3 Open Data Directive (PSI Directive).....	28
3.2 Privacy and Data Protection	30
3.2.1 GDPR Application	30
3.2.2 Key Roles and Responsibilities under the GDPR	38
3.2.3 Data Protection Principles	41
3.2.4 Legal Basis for processing Personal Data	43
3.2.5 Privilege for scientific Research.....	49
3.2.6 Safeguards for international Data Transfer.....	51
3.2.7 Anonymisation	53
3.2.8 Phased Approach to handle Personal Data	55
3.3 E-Privacy	56
3.3.1 Processing of Information	57
3.3.2 Dissemination	59
3.4 Security Aspects	60
3.4.1 Privacy related Security Aspects	61
3.4.2 Security Aspects under the Network Information Security Directive	63
4 Non-legal Aspects.....	66
4.1 Ethical Concerns	68
4.1.1 Interaction between Ethics and the Law	68
4.1.2 Non-legal Aspects of ethical Concerns	68

4.2	Fundamental Principles of Research Integrity	71
5	Conclusions.....	72

List of Figures

Figure 1 Relationship between the essential BE OPEN Deliverables leading to the Code of Conduct .	12
Figure 2 FAIR Principles in Relation to legal- and non-legal Issues for Open Science in Transport Research	14
Figure 3 Barriers to Data Re-Use assessed by BE OPEN Deliverable D 2.2	16
Figure 4 Barriers for producing Open/FAIR Data assessed by BE OPEN Deliverable D 2.2.....	17
Figure 5 Barriers for sharing Infrastructure assessed by BE OPEN Deliverable D 2.2	17
Figure 6 Overview on potential Aspects for legal Protection of Data.....	20
Figure 7 Definition of Personal Data under the GDPR	31
Figure 8 Interaction between technical Information / Statistics and Personal Data.....	32
Figure 9 Relative and absolute Approach of identifying a Natural Person	32
Figure 10 Guideline to qualifying Information as Personal Data	34
Figure 11 Territorial Scope of the GDPR	37
Figure 12 GDPR essential Data Processing Principles	41
Figure 13 Overview on legal Bases for processing Personal Data.....	44
Figure 14 Overview on phased Approach to handle Personal Data	56
Figure 15 Interlink between GDPR and e-Privacy Directive	59
Figure 16 Overview on adequate Implementation of Security Aspects.....	61

List of Tables

Table 1 Example for Interaction between Open Science and sensitive Data in Vehicle and Traffic Accident Databases	19
Table 2 Overview on Privacy Structures between multiple Controllers and/or Processors	40
Table 3 Overview on Privilege for scientific Purposes under the GDPR	51
Table 4 Transport Sector Modes covered by NIS Directive.....	65

Abbreviations and Terminology

ALLEA	European Federation of Academies of Sciences and Humanities
CJEU	Court of Justice of the European Union
CSIRT	Computer Security Incident Response Team
DMP	Data Management Plan
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EEA	European Economic Area
EOSC	European Open Science Cloud
EU	European Union
EU CFR	EU Charter of Fundamental Rights
FAIR	Findable, Accessible, Interoperable, Reusable
ICT	Information and Communication Technologies
IEC	International Electrotechnical Commission
IoT	Internet of Things
IPR	Intellectual Property Rights
ISO	International Standards Organisation
OES	Operators of Essential Services under the Network Information Security Directive
SCC	EU Commission Standard Contractual Clauses
US	United States of America
WIPO	World Intellectual Property Organisation

Executive Summary

The overarching vision of the BE OPEN project is creating a common understanding about the practical impact of Open Science, as well as identifying and putting in place the mechanisms to make it a reality in transport research. An essential element of reaching this vision through the BE OPEN project is developing a policy framework to establish and promote the ground-rules that will enable all stakeholders, existing tools and platforms, as well as resources and content to become an integral part of the Open Science in the transport research domain. This deliverable mainly outlines the essential legal issues and touches upon the fundamental principles of the main areas of Open Science in transport research. As such, it constitutes an important groundwork for the Code of Conduct on Open Science in Transport, which will also be developed by the BE OPEN project.¹

Sec 2 sets the scope for the subsequent analysis and puts the main legal issues and fundamental principles into context that have been determined by surveys in other BE OPEN deliverables as well as during the engagement of the BE OPEN project and on basis of a literature review.

Sec 3 constitutes the essential aspect of the deliverable, providing an easily accessible overview on important legal aspects for Open Science in transport research. The analysis of legal aspects serves to enable researchers and other stakeholders in transport research to determine legal issues and act appropriately. Furthermore, in assessing on these legal issues in preparation for the code of conduct, the challenges and opportunities are discussed, focussing on how research data should be treated in order to comply with statutory obligations based on EU directives and regulations as well as in light of CJEU judgements. These essential legal aspects are:

The legal protection of data through intellectual property rights: Based on the analysis of the key outcomes presented in other BE OPEN deliverables, the concept of data ownership materialises as a significant issue in the debate regarding data-sharing. Whereas data ownership does not yet exist as a legal concept in the EU Member States, legal protection of data, if only to a limited extent, is indeed afforded by intellectual property rights deriving from copyright, licensing, trade secrets and database rights. For Open Science in transport research, in particular, legal frameworks providing protection to databases are of relevance. Although databases are only eligible to legal protection under rather narrow prerequisites, and in particular, database-rights are materially not able to exceed to the protection immanent to the content of the database as such, the existing regulatory framework may pose a (legal) barrier for Open Science in transport research. Furthermore, the European legislator has recognised the need for stakeholders to access data on a broad scale, e.g. for research purposes and has therefore introduced exemptions that may facilitate Open Science in transport research among various areas and in numerous constellations. As a result, not only existing (legal) limitations but also the potential offered by the European legal framework facilitating the Digital Single Market are of immanent importance.

Privacy and data protection: Privacy and data protection have been identified as highly essential for Open Science in transport research. Most importantly, stakeholders must be able to identify the

¹ See BE OPEN deliverable D 4.4, “European Code of Conduct on Open Science in Transport”.

D4.1: Open Science in transport research: legal issues and fundamental principles

statutory obligations resulting from the processing of personal data. This requires a basic understanding about the key aspects of GDPR application, consisting of the territorial scope as well as the material scope, which largely leads to determining when an individual is identifiable. Turning towards the GDPR obligations, first the essential roles and responsibilities under the GDPR must be brought into context. This requires a description of aspects for the controller and/or processor qualification as well as information on mandatory privacy structures between multiple involved actors. Secondly, the basic data protection principles need to be closer assessed, since they constitute overarching requirements for all processing of personal data and have an important influence on the legal basis of processing personal data. Subsequently, the most important GDPR legal basis in the field of Open Science in transport research, consisting of consent, contractual necessity, legal obligations and legitimate interests are then explained and put into context. Since many activities in Open Science will qualify as scientific research, this is followed by an analysis of the existence and extent of a research privilege under the GDPR. Against the background of the international setting in Open Science, brief explanations are made on the requirements for data transfers outside the EU. The assessment on privacy and data protection is then closed by a proposed phased approach of avoiding the processing of personal data, inter alia, by means of data-anonymisation.

E-Privacy aspects: The legal privacy framework governing the processing of data is complemented by the e-Privacy Directive. In contrast to the GDPR, the scope of the e-Privacy Directive is considerably broader and does not only apply to personal data, but rather to all information regardless of the nature. Consequently, this setting requires an assessment of which processing activities may fall in the scope of the e-Privacy Directive and subsequently which particular requirements the e-Privacy Directive imposes on stakeholders with regard to these processing activities. Furthermore, where personal data are involved, the interaction between the GDPR and the e-Privacy Directive needs to be examined closely. Finally, in addition to certain processing operations, the e-Privacy Directive regulates electronic communication deemed as marketing-communication, which potentially affects dissemination strategies of various Open Science stakeholders.

Security Aspects: The security concerns determined in other BE OPEN deliverables are put into context and allocated to the respective EU legislation. The main security issues are again closely connected to data protection and privacy law. Notwithstanding, due to specific provisions and references to the transport sector, the relevance of the NIS Directive is further assessed before closing with a conclusion on corresponding security requirements under both the GDPR and the NIS Directive.

Sec 4 further addresses non-legal issues to Open Science in transport research. Apart from practical aspects in individual cases, this includes fundamental principles of research integrity as well as broader ethical concerns. These ethical concerns are in turns again often closely connected to legal aspects and need to be set into context. Likewise, through determining the fundamental principles of research activities, the interaction between these fundamental principles and the aforementioned legal issues can be further assessed. This leads to the conclusion that fundamental principles of research integrity can often conflict with legal aspects, especially in regards to privacy laws. Finally, given the importance of both legal and fundamental aspects, this conflict must be solved by a balancing of interests.

1 Introduction

1.1 Purpose of the Document

The BE OPEN project is a coordination and support action funded by the European Commission (“**EU Commission**”) in the Horizon 2020 research and innovation programme under the grant agreement No 824323. BE OPEN aims to promote Open Science in transport research and assist in regulating Open Science aspects and standardising them. The overarching vision of BE OPEN is to create a common understanding on the practical impact of Open Science and to identify and put in place the mechanisms to make it a reality in transport research. The main objectives of the BE OPEN project are:

- To develop a framework in order to establish a common understanding of operationalising Open Science in Transport.
- To map existing Open Science resources and see how transport research fits in.
- To facilitate an evidence-based dialogue to promote and establish Open Science in Transport.
- To provide the policy framework and guidance for Open Science implementation in transport.
- To engage a broad range of stakeholders in a participatory process for Open Science uptake.

The main purpose of the present deliverable D 4.1 is to determine the main legal issues as well as the fundamental principles of the main areas of Open Science in transport. This includes issues of data protection, Intellectual Property Rights (“**IPR**”), security aspects, ethical concerns, as well as privacy and other legal issues and aims for:

- Identifying the main legal issues as well as the fundamental principles of utilising Open Science in transport research.
- Assessing on legal issues of data protection, IPR, security aspects and privacy.
- Assessing on fundamental principles of research integrity (i.e. reliability, honesty, accountability) and their impact on ethical concerns and privacy.
- Identifying means to ensure high quality of Open Science resources by utilising and monitoring proper reliable methodologies and analytical tools in a transparent and fair way.
- Safeguarding accountability and transparent disclosure in the main areas of Open Science (i.e. Open Data, Open Software, infrastructure, Open Education and Open Citizen Science)

As such, this deliverable aims to constitute an important groundwork for the Code of Conduct on Open Science in Transport, which will be developed by the BE OPEN project in deliverable D 4.4.

D4.1: Open Science in transport research: legal issues and fundamental principles

Furthermore, the focus lies on outlining legal issues and barriers in an easily accessible way. This shall enable stakeholders to determine legal issues and react to them appropriately. The capability of identifying legal issues is an essential step to safeguarding the potential benefits of Open Science in transport research, which include effective and cost-saving research, unnecessary duplication of research and even the reduction of scientific fraud.

Contextually, the importance of these potential advantages can be seen in light of the recently published EU Commission communication on “A European strategy for data”². Here, the EU Commission outlines the rapidly growing volume of produced data from 33 zettabytes in 2018 to an expected 175 zettabytes in 2025 and sees this development as a major opportunity for the European Union (“EU”) to become a world leader in this area. Notwithstanding these positive effects, the EU Commission clearly points out legal guidelines by stating, *“in a society where individuals generate ever-increasing amounts of data, the way in which the data are collected and used must place the interests of the individual first, in accordance with European values, fundamental rights and rules.”*³

Hence, in determining legal issues and fundamental principles for Open Science in transport research, deliverable D 4.1 serves to safeguard the European values and fundamental rights and aims to insure the overarching objective that the human being is and remains at the centre of any innovation. Although this deliverable does not focus on providing solutions for the determined legal issues and such solutions will in fact usually depend on an assessment in each and every individual case, this document nevertheless does include indications of possible ways to avoid legal issues without prejudice to the code of conduct yet to be developed.

Notwithstanding, this document reflects the views of the authors for the academic purposes of the BE OPEN project and does not construe any legal advice third parties can rely upon.

Collecting transport research data from different modes of transport, different countries and touching upon sensitive data restrictions sets legal barriers. Such legal barriers are determined in this deliverable. In essence, they mainly originate from legal security aspects, legal protection of IPR and privacy aspects. The EU Commission is aware that there is an overarching need to standardise regional as well as international rules for data handling, including support from European legal regulation, covering security and privacy. In particular, data made available online should be ethically used, raising the importance of establishing mechanism to observe that the regulations are being followed. The EU Commission concludes in stating a concept under which data should be made *“as open as possible and as closed as needed”*.⁴

Apart from the legal barriers, there are also ethical issues, which include unintended secondary use, misappropriation and unequal distribution. Reaching effective standardised regional and international rules sufficiently lowering the existing legal and ethical barriers for Open Science is a time-consuming objective, which cannot easily be reached. In the absence of binding statutory regula-

² Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Document 52020DC0066, 19 February 2020.

³ Ibid.

⁴ European Commission, Directorate-General for Research & Innovation, “Guidelines on FAIR Data Management in Horizon 2020”, Version 3.0, 26 July 2016.

D4.1: Open Science in transport research: legal issues and fundamental principles

tions, a code of conduct can serve as effective measure to lower legal and fundamental barriers for Open Science in transport research. In order to develop such a code of conduct, the main legal and fundamental issues must first be determined and thoroughly analysed for their respective significance.

Emphasis will be given on the legal aspects of the main areas of Open Science in transport research. Further, of these legal aspects, especially privacy aspects will be highlighted, since the BE OPEN surveys have shown the importance amongst various stakeholders. Turning towards research-stakeholders, the European Data Protection Supervisor (“EDPS”) has recently recommended to intensify the dialogue between data protection authorities and ethical review boards. This is aimed at creating a common understanding of which activities qualify as genuine research, EU codes of conduct for scientific research, closer alignment between EU research framework programmes, data protection standards, and the beginning of a debate on the circumstances in which access by researchers to data held by private companies can be based on public interest.⁵ These aspects mentioned by the EDPS are indeed largely consistent with the key elements of BE OPEN Work Package WP 4. Not only does BE OPEN WP 4 aim at establishing a code of conduct for Open Science in transport research, rather the preliminary assessment of legal aspects carried out through this deliverable focusses exactly on the mentioned interaction between legal and fundamental (ethical) issues.

1.2 Methodology

This deliverable focusses on identifying the main legal issues in regards to Open Science through different resources and by a combination of legal methodological approaches. Determining existing legal issues is greatly subject to a descriptive research, describing the state of affairs, as it presently exists. In particular, this includes analysing the essential characteristics of present EU legislation. Furthermore, survey methods are added, not only by comparison of the law, but also by comparison of the results of other BE OPEN deliverables to the extent relevant to determine legal and fundamental issues in transport research. In order to cover abstract theory on how new EU regulations are likely to be implemented, conceptual analysis is added in regards to the analysis of the frameworks of EU directives and the potential new frameworks in the process of transposing the directives. Furthermore, this deliverable uses methods of evaluation in regards to how existing legislation practically affects stakeholders from their subjective views.

In regards to the sources and resources for deliverable D 4.1, the methodology follows a combined and layered approach, including the following resources:

- Legal and fundamental issues were first and ongoing determined in the BE OPEN project within the group of BE OPEN beneficiaries as experts in transport research. Essentially, BE Open beneficiaries were encouraged to report legal and fundamental issues they detected during their work in the project. In order to create awareness about potentially unanticipated legal issues amongst all beneficiaries during the entire duration of the project, the anticipated main aspects of deliverable D 4.1 were presented to all BE OPEN beneficiaries at an

⁵ European Data Protection Supervisor, “A Preliminary Opinion on data protection and scientific research”, edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf, last accessed 14 August 2020.

D4.1: Open Science in transport research: legal issues and fundamental principles

early stage of the project. In particular, this included guidance to determine essential legal issues by means of presenting guidance on the key legal aspects, such as the legal protection of data as intellectual property, differentiating between technical information on the one hand and personal data on the other hand, understanding to which extent scientific research-activity is privileged under EU privacy laws and raising awareness of e-Privacy aspects in terms of dissemination and/or communication with stakeholders.

- The BE OPEN project deliverables were analysed in order to determine direct legal references and hidden potential legal issues raised by participants in BE OPEN surveys conducted in the respective deliverables, and/or mentioned in the deliverable by the BE OPEN beneficiary. The results of these surveys are referenced in this deliverable and further analysed for their impacts on legal and fundamental issues, the most essential BE OPEN deliverables are mentioned in the figure below. In Particular, reports on legal and fundamental issues from various BE OPEN deliverables could be compared in order to safeguard and promote the validity of the answers.

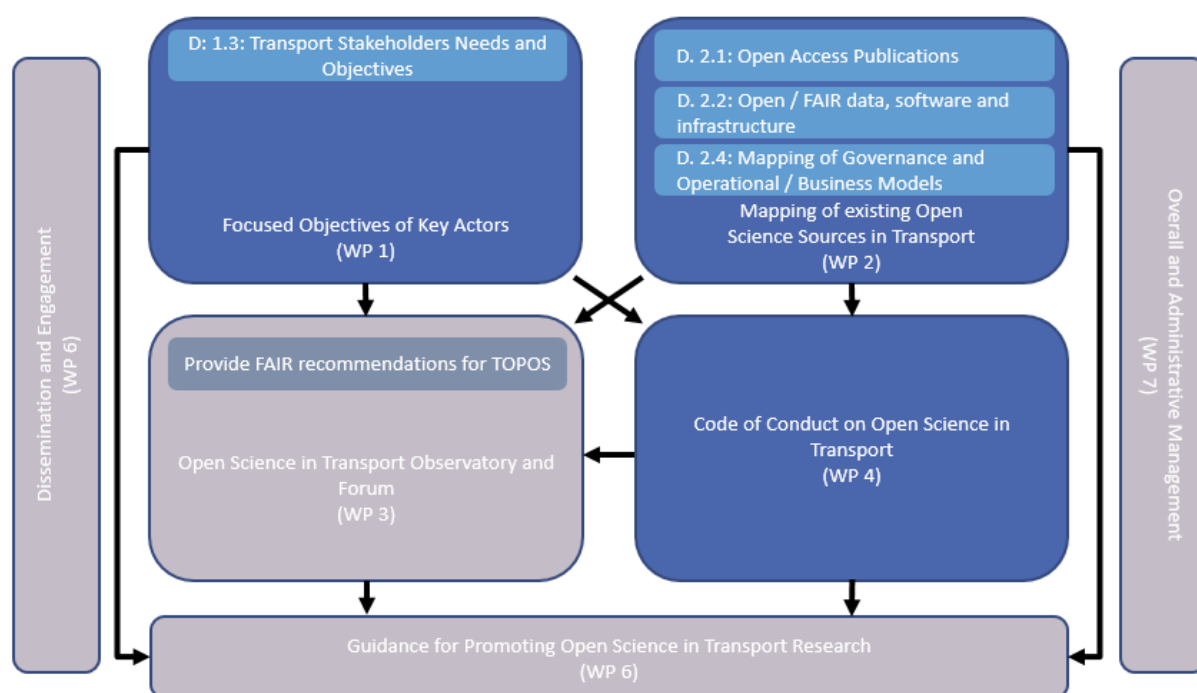


Figure 1 Relationship between the essential BE OPEN Deliverables leading to the Code of Conduct

- The European Open Science Cloud (“EOSC”) Rules of Participation and further EOSC related material is an important resource to determine legal and fundamental ideas. The EOSC is part of the European Cloud initiative and aims at developing high performance computing systems able to store and further process large amount of scientific data from EU projects. It will function as a free and open virtual environment to store, manage, analyse and re-use re-

search data across borders and scientific disciplines and contains a repository of documents holding information on potential legal and fundamental issues.⁶

- Literature review of relevant publications and legal research. In particular, the literature review was based on the repositories of publications, which have been determined in the BE OPEN project.⁷ The literature review was furthermore broadened by the sector-experience of Osborne Clarke as a law firm constantly involved in advising industry and policy-makers.

Rather than conducting a comparative legal review of all national laws regulating important legal issues for Open Science in transport research, this deliverable focusses on EU legislation, consisting of regulations, directives, decisions, recommendations and opinions.⁸

This approach is favourable due to the high level of harmonisation of the law in the EU. In particular, a comparative review of national EU Member State laws is largely unnecessary in regards to EU regulations, which are by definition binding in its entirety and directly applicable in all EU Member States. Likewise, if EU legislation is based on a directive, which needs to be transposed into EU Member State laws, the level of harmonisation is still considerably high due to the requirements for the transposition of the directive obliging EU Member States to choose the forms and means in such a way as to the practical effectiveness of the directive ("*effet utile*").⁹

Hence, in a pan-European context, a review of EU legislation is sufficient because the context of harmonisation in the EU follows the concept of mutual approximation of the national laws and administrative regulations of the EU Member States on basis of European legislation. This harmonisation relates to all areas of the law for which the EU has legislative powers, in particular applying to laws necessary to enforce the fundamental freedoms of the EU citizens.

2 Legal Issues and fundamental Principles

In order to identify the main legal issues as well as the fundamental principles of utilising Open Science in transport research, potential issues of data protection, IPR, security aspects and ethical concerns must be assessed in the spectrum of the fundamental principles of research integrity, i.e. reliability, honesty, accountability and respect.¹⁰ Since high quality Open Science resources require proper reliable methodologies and analytical tools as well as transparent and fair review, the fundamental principles of research integrity can conflict with legal issues, such as privacy aspects.

⁶ See European Commission on European Open Science Cloud, ec.europa.eu/research/openscience-/index.cfm?pg=open-science-cloud, last accessed 14 August 2020.

⁷ See i.e. BE OPEN deliverable D 2.1, "Open access publications and the performance of the European transport research".

⁸ Art 288 Para 2 Treaty on the Functioning of the European Union.

⁹ CJEU judgment of 15 July 1963 – C-34/62 ("Commission/Germany").

¹⁰ These fundamental principles are documented in: "The European Code of Conduct for Research Integrity", ec.europa.eu/research/participants/data/ref/h2020/other/hi/h2020-ethics_code-of-conduct_en.pdf, last accessed 14 August 2020, P 5.

D4.1: Open Science in transport research: legal issues and fundamental principles

For the purpose of the further assessment, “Open Data” is defined as data that can be freely accessed and further used, modified, and shared by anyone for any purpose¹¹. In particular, availability and access, re-use and redistribution of data, as well as universal participation are the key factors of Open Data.¹² The essential benefits of Open Data range from transparency and efficiency (e.g. allowing research to be reproduced) to increasing innovation in general. On an institutional level, European Open Data portals are available, with several EU countries having their own Open Data portal in place.¹³

For the purpose of the further assessment, “Open Science” is defined as making the primary outputs of publicly funded research results, research publications and the research data publicly accessible in digital format with no (or minimal) restriction as well as working on extending these principles of openness within the research community.¹⁴ In Open Science, data must be shared in such a way that both humans and machines are facilitated to access, as well as able to understand and re-use them. For that purpose, the FAIR Data Principles have been published as concise and measurable set of principles, aiming to act as a guideline in order to enhance the re-usability of data.¹⁵

As the following figure shows, these principle characteristics for research data are: Findability, Accessibility, Interoperability and Reusability. The main difference of Open and FAIR data involves the accessibility of the data. While both state that data should be as open as possible, FAIR data access can be restricted if necessary.¹⁶ This necessity can change according to the purpose or lifecycle of the data (e.g. during the research phase data is private, becoming public upon publication of the results).

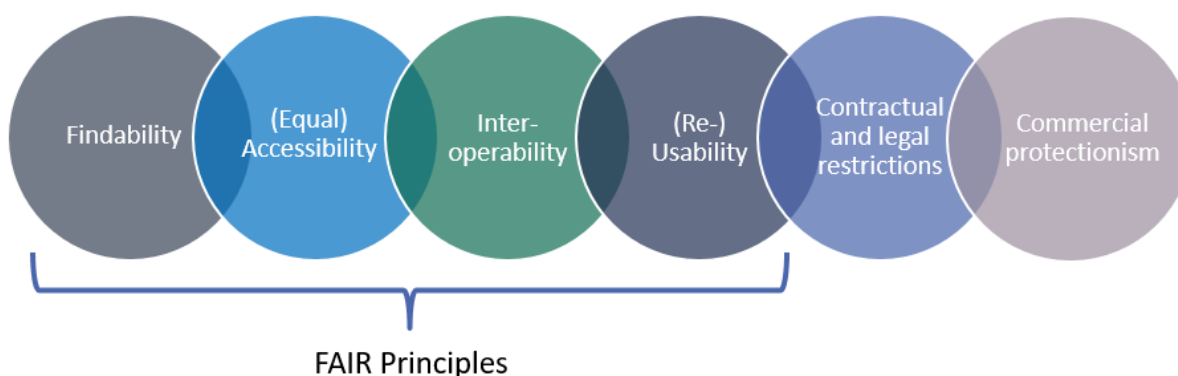


Figure 2 FAIR Principles in Relation to legal- and non-legal Issues for Open Science in Transport Research

In order to determine the main legal issues as well as the fundamental principles of the main areas of Open Science in transport research, it is important to face the specific Open and FAIR data opportunities and challenges in the transport research against the background of the characteristics of transport data.

¹¹ The definition for Open Data is derived from opendefinition.org, last accessed 14 August 2020.

¹² See opendatahandbook.org, last accessed 14 August 2020.

¹³ Examples for EU Portals are listed online data.europa.eu, last accessed 14 August 2020.

¹⁴ The definition for Open Science is derived from www.fosteropenscience.eu.

¹⁵ Wilkinson/Dumontier/Aalbersberg et al, “The FAIR Guiding Principles for scientific data management and stewardship”, doi.org/10.1038/sdata.2016.18, last accessed 14 August 2020.

¹⁶ www.go-fair.org/resources/faq/ask-question-difference-fair-data-open-data/.

D4.1: Open Science in transport research: legal issues and fundamental principles

For this purpose, “*Transport Data*” relates to a highly complex set of dimensions inherent to the transport sector. Amongst others, the several different transport modes (road, rail, water and air) serve as key feature, along with the respective variety of vehicles in every transport mode as well as the interrelated geographical data and connected infrastructure. To this end, the term Transport Data is characterised by a complex, multilevel topology, which corresponds to the various aspects of transport research, planning, design and operation, effectively translating into a high volume and variety of research data.¹⁷

BE OPEN surveys have concluded that Open and FAIR data in the transport research is packed with legal challenges, predominantly from the field of privacy law and data protection. However, the surveys also showed important (non-legal) fundamental issues for Open Science in transport research. These issues can be divided into several aspects in the data lifecycle.

Barriers to Re-Use of Open Data

The identified barriers for the re-use of data show a large repository for legal- and non-legal issues which in turns are connected to the fundamental principles of research integrity.¹⁸

In regards to non-legal issues, as the following figure shows, the assessment essentially displayed that:

- the sheer volume and variety of data used in the transport sector as such creates several issues in regards to storing, preserving, compiling or combining the transport data;
- technically, these issues are underlined by the fact that data collected for transport research or by governmental entities tends to be stored in distributed data silos which are subject to different ownerships and data formats. This in turns causes practical difficulties in light of cataloguing, finding, accessing and using research data;
- ethical, financial and commercial concerns as well as cultural barriers interact with the fact that the quality of data is insufficient and minimises the usefulness of the data.

In regards to legal issues, the survey has singled out the sensitiveness of data as main barrier to the Open and FAIR use of data. This sensitiveness of the data can be seen from different legal angles relating to

- (alleged) data ownership and issues of intellectual property rights;
- the protection of personal data through privacy and data protection laws;
- data security and access concerns which in turn may lead to detrimental effects of uncontrolled data access for safety and security.

¹⁷ BE OPEN deliverable D 1.2, “Open Science Framework Terminology and Instruments”, P 14.

¹⁸ BE OPEN deliverable D 2.2, “Open/FAIR data, software and infrastructure in European transport research”, P 25, figure 3.

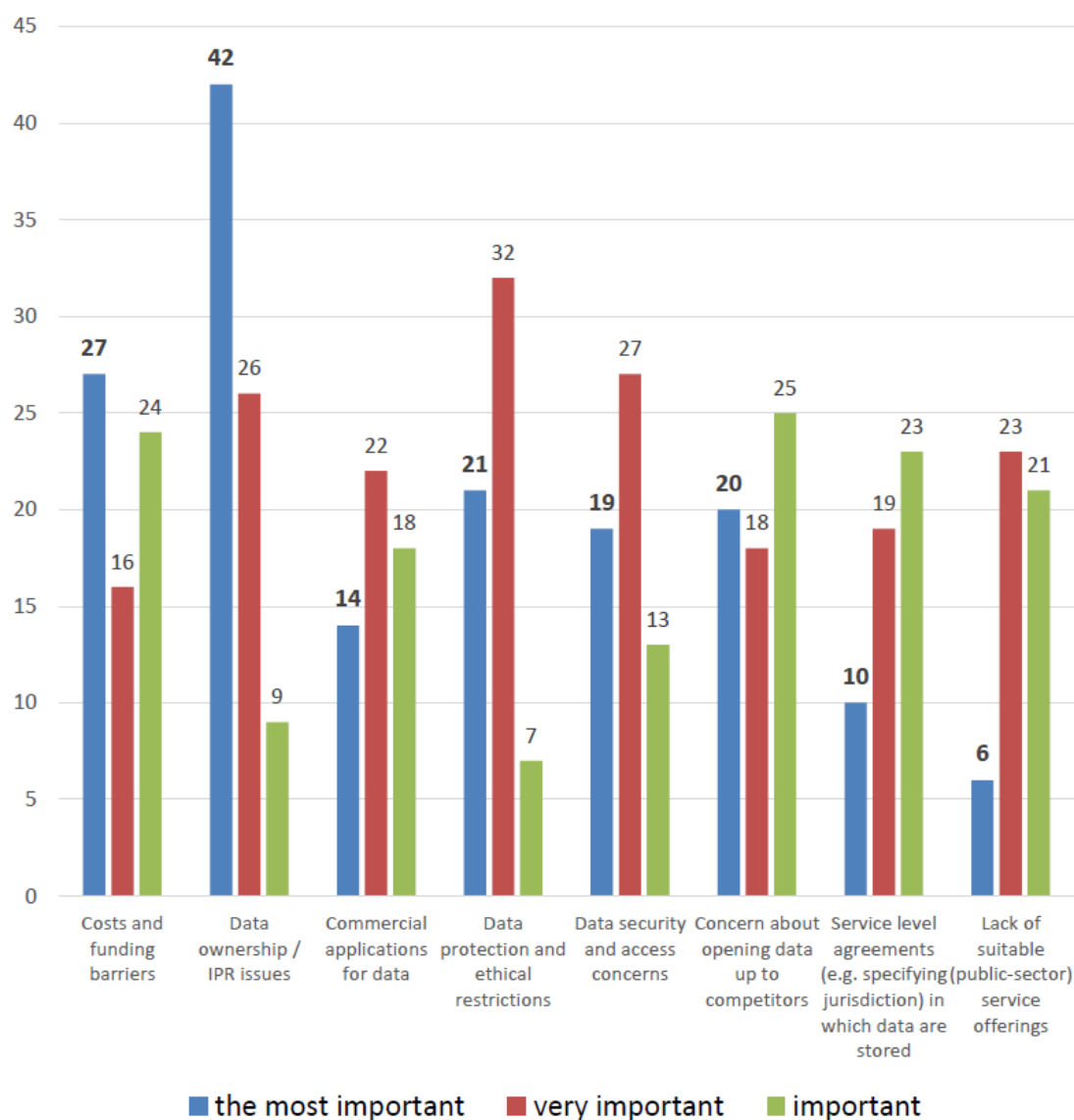


Figure 3 Barriers to Data Re-Use assessed by BE OPEN Deliverable D 2.2

Barriers for producing Open Data

Turning to the main barriers for producing data, as illustrated in the following figure, again legal aspects around privacy law and data protection are predominant. Legally, the outlined competitiveness of the organisation can relate to IPR issues as well as to underlying non-legal commercial aspects.¹⁹

¹⁹ Ibit, P 35, figure 8.

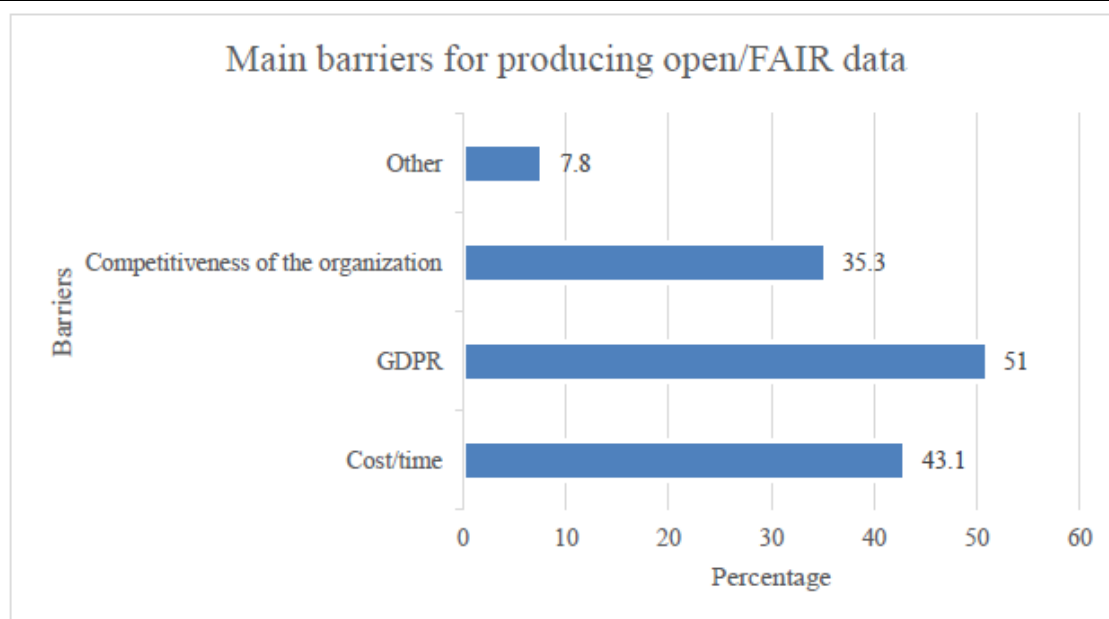


Figure 4 Barriers for producing Open/FAIR Data assessed by BE OPEN Deliverable D 2.2

Barriers for sharing Open Data Infrastructure

The picture is nearly similar when looking at the reasons why organisations do not share their open research infrastructure such as laboratories, computing systems, databases and models. According to the following figure illustrating the results of the BE OPEN survey, privacy aspects rank closely to the predominant competitiveness of the organisation.²⁰

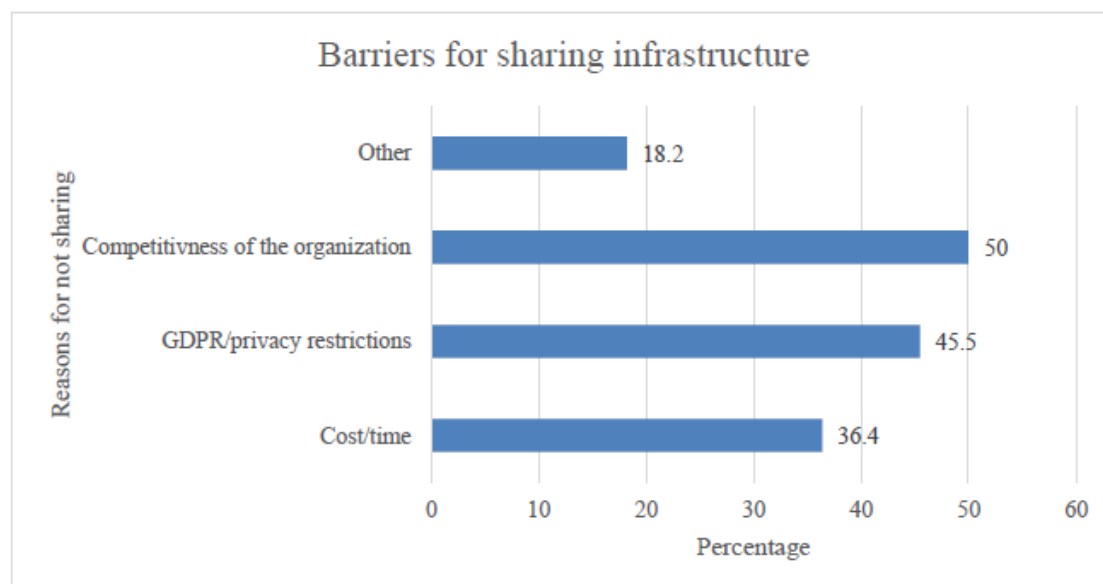


Figure 5 Barriers for sharing Infrastructure assessed by BE OPEN Deliverable D 2.2

²⁰ Ibit, P 35, figure 15.

In conclusion, different BE OPEN deliverables have focussed on various issues to Open Science in transport research with a strong focus on aspects determined as barriers for data sharing among researchers and the producers of data in general.²¹ Although the focus of these assessments varied in terms of stakeholders, transportation modes and countries, the outcome for the main legal issues as well as the fundamental principles are nearly identical. Essentially, the main barriers for Open Science in transport research can be found in both the competitive mind-set and the fear of not complying with privacy aspects, especially in light of the General Data Protection Regulation²² (“GDPR”).²³ Hence, these aspects touch local, national and international regulatory frameworks for legal data ownership and copyright on the one hand, and the need to protect personal data on the other hand. For the purpose of this assessment, the determined legal issues can be found in Sec 3 while non-legal issues and fundamental principles for Open Science in transport research are presented in Sec 4.

3 Legal Aspects

An essential aspect for Open Science in transport research is creating trust among stakeholders. Legally, the basis for this trust can be found in data protection and security of the data. Furthermore, key features include clear data protection rules which encourage stakeholders to use Open Science.²⁴

This urge to protect data obviously does not apply to all kinds of data. In fact, data may roughly be divided into sensitive and non-sensitive data. The legal issues determined in this deliverable refer to the sensitive category of data, which again are subject to further subdivision:

- **Personal data.** All personal data is considered sensitive data. Within the scope of personal data there is however room for further distinguishing categories of personal data by means of their sensitivity.²⁵ Notwithstanding this further distinction, all personal data remains sensitive data.
- **Proprietary data.** Proprietary data is considered sensible because unintentional revealing of the data can potentially harm an individual or a company both in terms of non-material or material detriments.

In order to balance the interests between utmost openness in Open Science and protection of data and individuals, a thorough analysis is required, carefully taking into account the protected interests in relation to research data in order to restrict access as little as possible while taking into account the varying sensitivity of personal and proprietary data.²⁶

²¹ Most prominently, BE OPEN deliverable D 2.4, “Governance and operational models” and BE OPEN deliverable D 2.2, “Open/FAIR data, software and infrastructure in European transport research”.

²² Regulation (EU) 2016/679.

²³ BE OPEN deliverable D 2.4, “Governance and operational models”, P 12.

²⁴ BE OPEN deliverable D 1.2, “Open Science Framework Technology and Instruments”, P 56.



²⁵ See special categories of personal in Art 9 Para 1 GDPR and personal data relating to criminal convictions and offenses in Art 10 GDPR for these highly sensitive categories of personal data.

²⁶ BE OPEN deliverable D 1.2, “Open Science Framework Technology and Instruments”, P 56; Gellerman/Svanberg/Barnard, “Data sharing of transport research data”.

D4.1: Open Science in transport research: legal issues and fundamental principles

As shown in the following table, Open Access to vehicle and traffic research accident databases serves as intuitive example on how Open Science interacts with sensitive personal- and proprietary data:

Table 1 Example for Interaction between Open Science and sensitive Data in Vehicle and Traffic Accident Databases

	<p>Open Access to vehicle and traffic research accident databases can be beneficial for Open Science in transport research.</p> <p>Research can help avoid accidents, which in turns saves money and even lives.</p>		<p>Open Access to vehicle and traffic research databases can lead to the processing of sensible data and be detrimental both in regards to personal data and proprietary data.</p> <p>Personal data: Identification of an individual through names, license plates or pictures, including indirect identification through a combination of sources.</p> <p>Proprietary data: Accident data can be used by insurance companies leading to higher prices for people living near accident black spots. Also Open Access to this data can be detrimental for professional accident-assessors who are no longer necessary to gather the information for insurances.</p>
---	--	---	--

The main legal aspects guiding the interaction between the benefits of Open Sciences in transport research and potential detriments for individuals, companies and/or society will be assessed in the following.

3.1 Legal Protection of Data (Intellectual Property Rights)

The analysis of the outcomes of other BE OPEN deliverables has shown that data ownership is a key issue in the debate regarding data-sharing and the exactitude and reliability of data. In fact, there even is a mind-set of data ownership amongst researchers believing that all produced data is actually exclusively owned by the respective researcher.²⁷

This legal interpretation of data ownership is somewhat astonishing against the background of a closer look at the EU Member State laws on the actual possibility of data ownership. It can be concluded that amongst many EU Member States the concept of data ownership is academically discussed but not yet existent as a legal concept.

²⁷ BE OPEN deliverable D 2.4, "Governance and operational models", P 36.

D4.1: Open Science in transport research: legal issues and fundamental principles

- In **France**, there are no laws specifically directed to an ownership right over data. The French civil code merely does apply both civil and criminal law mechanisms providing the holder of data with the ability to prevent or restrain the misuse of data.²⁸
- In **Germany**, there is no established ownership or other erga-omnes right in data. However, data is protected by various statutes under criminal law and the case law confirms that accessing data of another company can constitute a violation of trade and business secrets.²⁹
- In **Italy**, there is no concept of data ownership but rather only certain means of data protection under intellectual property aspects.³⁰
- In the **Netherlands** and in **Belgium**, there is no ownership of data but rather only protection

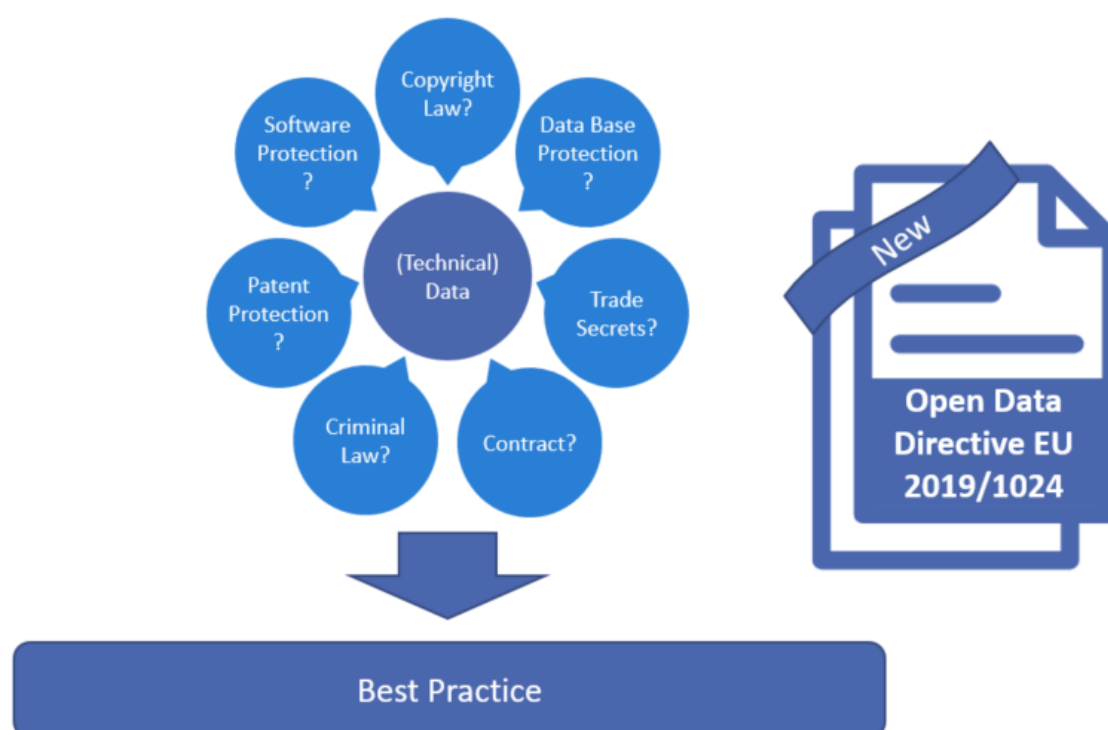


Figure 6 Overview on potential Aspects for legal Protection of Data

of databases and software.³¹

Turning away from this narrow view on data ownership, the focus should rather be on the existing limited scope of legal protection of data in the EU. Most common legal instruments to exclude others of using data are the intellectual property rights derived from copyright, licensing, trade secrets and database rights. Each of these instruments may on the one hand promote Open Science and on the other hand lead to detrimental effects of data protectionism. Corporate secrecy, particularly in the

²⁸ EU Commission study 30-CE-08065500/00-95, "Legal study on Ownership and Access to Data", P 43.

²⁹ Ibid, P 43.

³⁰ Ibid, P 134.

³¹ Ibid, P 143, 145.

tech-sector, which controls the most valuable data for understanding the impact of digitisation and specific phenomena like the dissimulation of misinformation, is a major barrier to Open Science.³²

All EU Member States are among the members of the World Intellectual Property Organisation (“WIPO”) and have signed up to the Berne Convention, aiming to protect the rights of authors in their literary or artistic works. The legal framework governing intellectual property rights in relation to open access to research data references both moral rights and exploitation rights for the researchers or institutions who created, collected or curated the data.

Notwithstanding, against the background of various different IPR regimes in and outside the EU, neither of these effects are deemed absolute, since in an international context, IPR can only provide a relatively limited scope of protection. Furthermore, the BE OPEN surveys have shown that there are different levels of competitiveness across different fields of research. Climate research, which predominantly is based on local data, for instance has a long-standing culture for sharing data.³³ The relevant data for the transport sector however predominantly originates from companies that are not willing to share data openly to everyone due to competitive advantages. In fact, even research institutes are to a certain stage competitive, e.g. when it comes to gaining new projects.³⁴

By definition, intellectual property rights protect the work of an individual that is the result of creativity, innovation, skill and specialist effort. The associated intellectual property rights can be divided into moral rights on the one hand and exploitation rights on the other.

- Moral rights are usually non-transferrable and include entitlements to attribution for the work, or even merely the right to remain anonymous. With regard to such moral rights, not only rights of attribution, but also aspects of respecting the integrity of the original work are implicated.
- Exploitation rights are usually transferrable and include the entitlement to reproduce, distribute, perform, broadcast or transform materials without any permission. These rights are closely related to aspects of open access to research data by means of copyright, database rights, trade secrets, patents, licenses and in addition rights allowing for reproduction, distribution and transformation of materials.

Even individuals or entities, such as private organisations may be eligible to protection by so called “neighbouring” or “related” rights, even if they have not created the data but rather only collected or arranged it in a systematic or methodical way. Such intellectual property rights include, in particular copyright, trade secrets and database rights; each of which will be discussed in more detail below.

3.1.1 Copyright

Copyright forms a significant component of intellectual property rights and can be described as the exclusive right of an author of a work (e.g., literature, science, arts), to determine where, when and

³² European Data Protection Supervisor, “A Preliminary Opinion on data protection and scientific research”, edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf, last accessed 14 August 2020.

³³ BE OPEN deliverable D 2.4, “Governance and operational models”, P 37.

³⁴ BE OPEN deliverable D 2.4, “Governance and operational models”, P 37.

D4.1: Open Science in transport research: legal issues and fundamental principles

how the work is made available to the public and further used by others. Copyrights are significant legal barriers when they restrict the usage of the works created as a result of research, regardless of whether this refers to research data held by researchers, institutions or publishers.

Essentially, copyrights include two sets of rights³⁵:

- Economic rights enabling the holders of the rights to both control the use of their works and essentially gain remuneration for the use of the work by others. Economic rights normally take the form of exclusive rights, notably to authorise or prohibit the making and distribution of copies as well as communication to the public. At EU level, these economic rights and their terms of protection are harmonised.
- Moral rights include the right to claim authorship of the work and the right to object to any derogatory action in relation to the work. They are not harmonised at EU level.

Licensing constitutes the main mechanism for the exercise of copyright and related rights. Depending on the relevant right as well as the type of use and the sector, licences are commonly granted directly by the holder of the right or collective management organisations. On a related note, the EU has recently adopted legislation to improve the functioning of collective management organisations including through facilitating the provision of multi-territorial licences.

Essentially, copyright protection is available to databases and database rights grant further protection. Even though existing provision affording protection for databases are not comprehensive and in case of database rights do not exceed to the content of the database as such, the existing regulatory framework may very well pose a (legal) barrier for Open Science in transport research and should therefore be addressed closely.

3.1.1.1 Databases as a “Work”

Since all electronic information is treated in copyright law as a written (literary) work, copyright is, in principle afforded to the content of databases as a compilation of data as such. However, because in modern electronic databases the selection and arrangement of the contents is unlikely to have been the subject of significant skill and judgment, databases will most likely not meet the required standard to qualify as a “work”. This applies in particular to databases compiled through the automatic capture and collation of data.³⁶ In order fall within the scope of protection granted by copyright under the Directive on the harmonisation of certain aspects of copyright and related rights (“**InfoSoc Directive**”)³⁷, a database has to meet the qualifying criteria of a “work”. For such qualification and equally to other literary works, databases have to reach a minimum standard of creativity, allowing for the conclusion that they are the author’s own intellectual creation.³⁸ Copyright is therefore restricted to works where some sort of value has been added by the exercise of creative or at least

³⁵ See EU Commission on Copyright, ec.europa.eu/digital-single-market/en/copyright, last accessed 14 August 2020.

³⁶ EU Commission study 30-CE-08065500/00-95, “Legal study on Ownership and Access to Data”, P 13

³⁷ Directive 2001/29/EC.

³⁸ CJEU judgement of 16 Juli 2009 – C5/08 (“Infopaq”), Rec 31 et seq.

intellectual judgment.³⁹ Thus, if at all, the InfoSoc Directive is only capable of providing very limited protection to data itself.

3.1.1.2 Database Directive

Supposedly due to the aforementioned aspects, historically, not all EU Member States afforded copyright protection to databases. To ensure and harmonise such protection in the EU, the European legislator introduced the Directive on the legal protection of databases (“**Database Directive**”)⁴⁰.

The Database Directive applies to all databases marketed in the EU, satisfying the criteria laid down in Art 1 Para 2 Database Directive. In accordance with this provision, a database must be a collection of independent works, data or other materials which:

- are arranged in a systematic or methodical way; and
- are individually accessible by electronic or other means.

The Database Directive then distinguishes between a genuine copyright for databases meeting the criteria of Art 3 Database Directive and a database right *sui generis* for databases pursuant to Art 7 Database Directive.

3.1.1.3 Copyright for Databases

Art 3 Para 1 Database Directive obliged the Member States to establish copyright protection for databases allowing for the conclusion of being the author’s own intellectual creation through a unique selection or arrangement of the content.⁴¹ While, Art 3 Database Directive refers to the criteria mentioned above in Sec 3.1.1.1, it limits the protection to the structure of the database, which in turns falls under the scope of protection to the extent it is considerably “original”⁴² and explicitly excludes the content of the data.⁴³ The criterion of originality applies to a database, “*when, through the selection or arrangement of the data which it contains, its author expresses his creative ability in an original manner by making free and creative choices*”. By contrast, that criterion is not satisfied when the set-up of the database is dictated by technical considerations, rules or constraints, which in turns leave no room for creativity.⁴⁴

Expending significant labour and skill in compiling a database will not be considered sufficient to give rise to copyright protection under Art 3 Para 1 Database Directive, unless the author has also expressed creative originality in the selection or arrangement of the data contained in that database (whether carried out by hand or by software). Modern electronic databases are therefore rarely likely to qualify under this threshold.⁴⁵

³⁹ CJEU judgement of 4 October 2011 – C-403, 429/08 (“Football Association Premier League Ltd”), Rec 98; CJEU judgement of 1 December 2011 – C-145/10 (“Painer”), Rec 88 et seq.

⁴⁰ Directive 96/9/EC.

⁴¹ See also Recital 15 Database Directive.

⁴² CJEU judgement of 1 March 2012 – C-604/10 (“Football Dataco”), Rec 32 et seq.

⁴³ Recital 15 Database Directive.

⁴⁴ CJEU judgement of 1 March 2012 – C-604/10 (“Football Dataco”), Rec 38 et seq.

⁴⁵ EU Commission study 30-CE-08065500/00-95, “Legal study on Ownership and Access to Data”, P 13.

Where the database is eligible for copyright protection, the database owner is then vested with a property right allowing the databases' author to assign, mortgage or license the copyright. In addition, Art 5 Database Directive stipulates the author's right to prevent temporary or permanent reproduction by any means and in any form, in whole or in part; unauthorised alteration, reproduction or distribution of the contents of the database.

3.1.1.4 *Sui Generis Right*

In addition to copyright protection, the Database Directive obliges EU Member States to grant databases protection in form of a database right *sui generis* under certain prerequisites. This database right *sui generis* applies equally to databases that do not satisfy the criteria mentioned above and therefore are not subject to protection under copyright as well as such databases eligible to protection by copyright or by other rights.

The purpose of the *sui generis* right is to provide the maker of a database with protection, limited in time and scope, ultimately aiming at securing the investment involved in creating the database. In this respect, the substantial investment made through the construction of the database is a central prerequisite for protection under the *sui generis* right. Accordingly, Art 7 Para 1 Database Directive requires a qualitatively and/or quantitatively substantial investment in either the obtaining, verification or presentation of the content of the database concerned.⁴⁶ The limitation stating that only investments connected to the procurement, verification or presentation of the database content can establish *sui-generis* protection, establishes a distinctive restriction, excluding in particular consideration of investments in generating data. Hence, only investments serving to identify and search for existing independent sets of data and collect them in the database are taken into account. On the contrary, investments used to create the elements of which the content of a database consist in the first place, are deemed to remain disregarded. The reason for this differentiation is closely connected to the aim of protecting the investment by the *sui generis* right created by the Database Directive. In particular, the objective is solely limited to encouraging the establishment of systems for storing and processing existing information and shall not directly encourage the creation of material elements aimed to be assembled in a database.⁴⁷ The qualitative or quantitative investment must further reach a certain threshold with regard to financial, human or technical resources in order to be considered "substantive". However, the precise meaning of substantive remains unclear.⁴⁸

Art 7 Database Directive provides for the right of the maker of a database to prevent third parties from extracting and/or re-utilising whole or substantial parts of the content of the database, or repeatedly and systematically extracting or re-utilising insubstantial parts of the database. Thus, without permission, third parties may neither permanently or temporarily transfer all or a substantial part of the content of a database to another medium by any means or in any form, nor make the

⁴⁶ *Hermes*, Wandtke/Bullinger, "Urheberrecht", § 87a, Rec 33.

⁴⁷ CJEU judgement of 9 November 2004 – C-203/02 ("The British Horseracing Board Ltd"), Rec 31, 42; CJEU judgement of 9 November 2004 – C338/02 ("Football Fixture Lists I"), Rec 24; CJEU judgement of 9 November 2004 – C-422/02 ("Football Fixture Lists II"), Rec 40; CJEU judgement of 9 November 2004 – C-46/02 ("Football Fixture Lists III"), Rec 31 et seq.

⁴⁸ *Hermes*, in: Wandtke/Bullinger, "Urheberrecht", § 87a, Rec 34.

D4.1: Open Science in transport research: legal issues and fundamental principles

content of the database available to the public, by means of distributing copies or any form of transmission.

However, turning towards expiration dates, such protection is temporary limited to 15 years from the end of the calendar year in which the database was completed. Notwithstanding, where updates to the database amount to a substantial change of content, it is likely that the updated database qualifies for its own 15-year term of protection. As a result, the right can therefore last indefinitely, as long as the database is updated periodically and substantially.⁴⁹

Further restriction with regard to the scope of the right are laid down in Art 8 Database Directive, essentially aiming at rights and obligations granted to lawful users of a public database. In essence, the maker of a public database is as such not entitled to prevent lawful database-users from extracting and/or re-utilizing insubstantial parts of its contents, evaluated qualitatively and/or quantitatively, for any purposes whatsoever. This restriction, effectively, takes away control from the maker of the database once the database was made public, e.g. in the course of commercial licensing.

3.1.1.5 Copyright Directive

A new development was introduced by the Directive on copyright and related rights in the Digital Single Market ("**Copyright Directive**")⁵⁰. The Copyright Directive entered into force on 6 June 2019 and amends both the Database Directive and InfoSoc Directive. Its provisions shall be transposed by the EU Member States until 7 June 2021.

Essentially, the copyright rules provided by Art 3 and 4 of the Copyright Directive are of potential relevance for Open Science in transport research. In fact, Art 3 Para 1 requires EU Member States to establish exceptions in their regime for copyright and database rights applying to reproductions and extractions made by research organisations in order to carry out text and data mining of works or other subject matter to which they have lawful access for the purposes of scientific research. These exceptions aim at allowing researchers linked to a university or another research organisation to analyse text and data on a large scale by means of automated analytical techniques. In essence, this exemption provides for the possibility to analyse text and data in a digital form in order to generate information such as patterns, trends and correlations.⁵¹

A more extensive exemption with regard to the personal scope is provided by Art 4 Copyright Directive for reproductions and extractions of lawfully accessible works and other subject matter for the purposes of text and data mining in general. However, it applies only under the condition that the use of works and other subject matter has not been expressly and appropriately reserved by the rightholders.

In conclusion, both provisions stipulate certain restrictions. The broader exemption of Art 3 Copyright Directive, for one, applies only to research organisations, which are defined as universities, re-

⁴⁹ EU Commission study 30-CE-08065500/00-95, "Legal study on Ownership and Access to Data", P 15.

⁵⁰ Directive (EU) 2019/790.

⁵¹ European Data Protection Supervisor, "A Preliminary Opinion on data protection and scientific research", P 11, edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf, last accessed 14. August 2020.

D4.1: Open Science in transport research: legal issues and fundamental principles

search institutes or other entities, primarily engaged in scientific research or educational activities, which involves the conduct of scientific research. Further these organisations have to carry out the aforementioned activities either on a non-profit basis or by re-investing all of the profits into scientific research. As an alternative, the exemptions also apply to organisations that are recognised by a EU Member State pursuant to a public interest mission.⁵² Thus, at least the rather broader provision excludes all stakeholders that are either individual researchers and most organisations controlled by private undertakings.⁵³ Furthermore, the criterion of lawful access aims at restricting the application to content already accessible by these organisations based on an open access policy or through contractual arrangements, where however the terms of the licences exclude text and data mining.⁵⁴ Essentially, the application of the general exemption of Art 4 Copyright Directive seems to be restricted to content that is freely available online and not protected by technical or other means against data mining.⁵⁵

Consequently, even though the scope of these exemptions is rather limited, they may facilitate Open Science in transport research in various areas and constellations. Thus, an overall positive effect for Open Science can be expected.

3.1.2 Trade Secrets

Other than aiming at controlling who uses works through copyright and database rights, trade secrets protection aims at keeping commercially valuable information confidential. At first sight, this commercial aspect can lead to the false conclusion, that trade secrets are only relevant in a commercial capacity amongst (commercial) industry stakeholders. However, the BE OPEN surveys have clearly outlined, that non-commercial research institutes in fact are to a certain stage competitive and necessarily are engaged in commercial activities such as raising funds for research projects.⁵⁶

Hence, trade secrets can pose important barriers to Open Science in transport research because researchers develop commercially valuable information in the course of their activities, and treat this information as confidential in order for them to have a competitive advantage.⁵⁷ Essentially,

- the information can be of a technical nature (e.g. manufacturing process or software) or commercial nature (e.g. list of potential funding leads), and
- it can be strategic, long-term knowledge (e.g. blueprint for technical innovation), or more short-lived (e.g. the price offered in a bidding procedure).

⁵² Art 2 No 1 Copyright Directive.

⁵³ European Data Protection Supervisor, “A Preliminary Opinion on data protection and scientific research”, P 11, edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf, last accessed 14. August 2020.

⁵⁴ Recital 10, 14 Copyright Directive.

⁵⁵ Recital 14, 18 Copyright Directive.

⁵⁶ BE OPEN deliverable D 2.4, “Governance and operational models”, P 37.

⁵⁷ See European Commission, “FAQ: Protection against the unlawful acquisition of undisclosed know-how and business information (trade secrets)”, ec.europa.eu/growth/industry/intellectual-property/trade-secrets/faq_en, last accessed 14 August 2020.

D4.1: Open Science in transport research: legal issues and fundamental principles

While regionally, trade secret protection has traditionally been implemented in the field of competition law and employment law, the globalised world calls for trade secret protection on a global scale. Internationally, there is a long history of attempts to harmonise the legal protection for trade secrets. Initially, trade secret protection was first internationally ensured by the Agreement on Trade-Related Aspects of Intellectual Property Right (“TRIPS Agreement”), which introduced a definition for “undisclosed information”⁵⁸ which has been adopted by the Directive on the protection of undisclosed know-how and business information (“**European Trade Secret Directive**”)⁵⁹ As such, the directive applies to information meeting all of the following requirements:⁶⁰ The information

- is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among- or readily accessible to persons within the circles that normally deal with the kind of information in question,
- has commercial value because it is secret, and
- has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret.

Hence, in essence, trade secrets are defined as commercially valuable pieces of information, which are not generally known among experts in the field and have been subject to reasonable steps in keeping them a secret by the holder of the secret. To clarify, also data can fall under this definition and is eligible of being protected as a trade secret as long as it remains a secret. Hence, once the dataset is disclosed, the protection can no longer be claimed.

Commonly, trade secrets are an essential element of innovative processes leading to legally protected intellectual property rights such as a copyright. However, contrary to popular belief, trade secrets are by virtue not an intellectual property right. In fact, the holder of a trade secret does not have an exclusive right over its creation and cannot prevent competitors from copying and using the same solutions. This becomes clear when taking into account that reverse engineering by discovering the technological principles of a device, object or system through analysis of its structure, function and operation is lawful. In conclusion, trade secrets are only legally protected in instances where someone has obtained the confidential information by illegitimate means (e.g. through spying, theft or bribery).⁶¹ Hence, legally, trade secrets should be considered an addition to intellectual property rights, which exists as long as the conditions for trade secret protection remain fulfilled.

Most importantly, the directive harmonises the legal means enabling victims of trade secret misappropriation to seek protection. Apart from claims for damages, they consist of injunctions and corrective measures, which can be summarized as follows:⁶²

⁵⁸ Art 39 Para 2 TRIPS Agreement.

⁵⁹ Directive (EU) 2016/943.

⁶⁰ Art 2 Para 1 Trade Secret Directive.

⁶¹ See European Commission, “FAQ: Protection against the unlawful acquisition of undisclosed know-how and business information (trade secrets)”, ec.europa.eu/growth/industry/intellectual-property/trade-secrets/faq_en, last accessed 14 August 2020.

⁶² Art 12 Trade Secret Directive.

D4.1: Open Science in transport research: legal issues and fundamental principles

- The cessation of or, as the case may be, the prohibition of the use or disclosure of the trade secret.
- The prohibition of the production, offering, placing on the market or use of infringing goods, or the importation, export or storage of infringing goods for those purposes.
- The destruction of all or part of any document, object, material, substance or electronic file containing or embodying the trade secret or, where appropriate, the delivery up to the applicant of all or part of those documents, objects, materials, substances or electronic files.
- The adoption of the appropriate corrective measures with regard to the infringing goods through
 - recall of the infringing goods from the market,
 - depriving the infringing goods of their infringing quality, and/or
 - destruction of the infringing goods or, where appropriate, their withdrawal from the market, provided that the withdrawal does not undermine the protection of the trade secret in question.

In conclusion, trade secrets can be a serious barrier for Open Science in transport in cases where protected information is unlawfully obtained and used. Hence, all use of information is eligible of posing a risk to the extent it has been unlawfully obtained. This is the case if the concerned individual knew, or ought, under the circumstances to have known that the trade secret was unlawfully disclosed because it was acquired or used by means of

- unauthorised access to the information (e.g. unauthorised copying of information), and/or
- in breach of a confidentiality agreement or other legal obligation to not disclose the licensing.

3.1.3 Open Data Directive (PSI Directive)

In light of the aforementioned barriers for available data in the field of Open Science in transport research, and against the background that corporate companies growingly determine how and where information flows, the Directive on Open Data and the re-use of public sector information ("**Open Science Directive**")⁶³ can be of importance for Open Science in transport research. In particular, by facilitating access to public information in the transport sector. The Open Science Directive entered into force on 16 July 2019 and needs to be transposed to EU Member State law by 17 July 2021.⁶⁴ The new directive replaces the Public Sector Information Directive ("**PSI Directive**")⁶⁵, which has been in force since 2003 and was subsequently amended in 2013⁶⁶.

⁶³ Directive (EU) 2019/1024.

⁶⁴ Art 17 Para 1 Open Science Directive.

⁶⁵ Directive 2003/98/EC.

⁶⁶ Amended by the Directive 2013/37/EU.

D4.1: Open Science in transport research: legal issues and fundamental principles

The EU Member State laws transposing the PSI Directive focus on the economic aspects of the re-use of information rather than on access to information by citizens. The directive addresses material held by public sector bodies in the EU Member States, at national, regional and local levels, including ministries, state agencies and municipalities, as well as organisations largely controlled or funded by public authorities. While covering written texts, databases, audio files and film fragments, the PSI Directive does not apply to the educational, scientific and broadcasting sectors.

With the new Open Science Directive and the yet to be established EU Member State laws transposing the directive, a new framework shall be established aiming at promoting the re-use of public and publicly funded information to facilitate innovation through exploitation of public sector information as a source of digital innovation.⁶⁷

In essence, the new prospective laws on basis of the Open Science Directive are aimed at:

- stimulating the publishing of dynamic data and the uptake of Application Programme Interfaces (APIs),
- limiting the exceptions currently allowing public bodies to charge more than the marginal costs of dissemination for the re-use of their data,
- strengthening the transparency requirements for public–private agreements involving public sector information, avoiding exclusive arrangements, and
- enlarging the material scope of the directive to
 - data held by public undertakings, under a specific set of rules, and
 - research data resulting from publicly funded research. Furthermore, policies for open access to publicly funded research data shall be developed and the re-usability of research data that is already contained in open repositories shall be facilitated.

Highly relevant for Open Science in transport research, the Open Data Directive requires the adoption of a list of high-value datasets to be provided free of charge. Most importantly for the transport sector, amongst these datasets listed in Annex 1 of the Directive are mobility datasets.⁶⁸ Notwithstanding, there are limits to the openness under the revised EU Commission Recommendation on access to and preservation of scientific information referring to the principle that research data should be “as open as possible, as closed as necessary”.⁶⁹

⁶⁷ Schweitzer, “Datenzugang in der Datenökonomie: Eckpfeiler einer neuen Informationsordnung, Gewerblicher Rechtsschutz und Urheberrecht”, GRUR 2019, 572.

⁶⁸ Open Science Directive, Annex 1 No 6.

⁶⁹ European Commission, Recommendation (EU) 2018/790 of 25 April 2018 on access to and preservation of scientific information C(2018) 2375, eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018H0790, last accessed 14 August 2020.

3.2 Privacy and Data Protection

The BE OPEN surveys conducted in various deliverables showed that privacy aspects and especially the GDPR rank top in terms of legal issues for Open Science in transport research. Primarily, this is likely the effect of privacy aspects becoming more prominent in the open public. This in turns is most likely a consequence of the drastic GDPR fines of up to EUR 20,000,000 or 4% of a company's total annual worldwide turnover for violations.

Europe is widely considered as a global pioneer in data protection and privacy.⁷⁰ As EU regulation, the GDPR is directly applicable in all EU Member States pursuant to Art 288 Para 2 Treaty on the Functioning of the European Union. It thus takes precedence over all national provisions, unless opening clauses allow for deviations or more specific national laws. Notwithstanding, the following assessment on the territorial scope of the GDPR will show that the GDPR furthermore indirectly applies far beyond the borders of the EU.

Privacy aspects are of vital importance for all data related research activities because within the scope of the GDPR, any processing of personal data is generally prohibited and will only be deemed permissible if there is a valid legal basis specifically applicable to the processing activity. Digitisation has made generating and disseminating personal data easier, faster and cheaper and has transformed traditional means of carrying out research. Furthermore, the boundary between private sector research and traditional academic research is blurrier than ever, making it significantly harder to distinguish research with generalisable benefits for society from that which primarily serves private interests.⁷¹ Therefore, the GDPR generally applies similarly to all research stakeholder, whilst acknowledging that certain research is indeed carried out within an established framework of professional ethical standards. The however does not influence the GDPR scope of application and will be treated separately in Sec 3.2.5.

3.2.1 GDPR Application

The application of the GDPR is dependent on the material and territorial scope of each and every processing activity.

3.2.1.1 *Material Scope (Qualification of Data as personal)*

The rules for determining the material scope of the GDPR can be found in Art 2 GDPR. Most importantly, the GDPR only applies to the processing of personal data within the meaning of Art 4 No 1 GDPR.

Qualification of Information as Personal Data

The assessment of whether or not information qualifies as personal data or not is amongst the most important tasks for anyone dealing with data in a professional context. Against the background of the

⁷⁰ Griegerich, "Europäische Vorreiterrolle im Datenschutzrecht: Neue Entwicklungen in der Gesetzgebung, Rechtsprechung und internationalen Praxis der EU", ZEuS 2016, 301, 342.

⁷¹ See European Data Protection Supervisor, A Preliminary Opinion on data protection and scientific research, P 2, edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf, last accessed 14 August 2020.

D4.1: Open Science in transport research: legal issues and fundamental principles

widespread fear of sharing personal data amongst stakeholders in the transport sector, it can be concluded, that the real risks do not arise from the processing of personal data itself, but rather from processing data without noticing that the data qualifies as personal data. In such a case, where someone is not aware of the fact that processed data qualifies as personal, there is no chance to comply with the mandatory requirements of the GDPR.

Hence, it is an essential task for all stakeholders working with data, to continuously keep in mind that all data may potentially be referenced to a natural person and thus qualify as personal data. The following figure outlines the definition for personal data in the GDPR.

Article 4

Definitions

For the purposes of this Regulation:

- (1) ‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one 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;

Figure 7 Definition of Personal Data under the GDPR

While any form of direct identification (e.g. through a name) is usually an evident case of personal data, determining the indirect identifiability of a natural person by a piece of information can be very challenging.

In essence, an individual is identifiable if the information at hand is not sufficient in itself to be referenced to an individual, but this reference can be achieved as soon as the information is linked to other information. Here all means need to be taken into account that are likely to be used by the person or entity involved in the processing as well as any other person that is likely to actually identify the individual directly or indirectly.⁷² According to Recital 26 GDPR, the question as to which means are likely to be used for identification must be based on all information known or ascertainable about the concerned individual and all objective factors, such as the costs of identification and the time required for this. Hence, means can be disregarded to the extent they would make an identification practically impossible, e.g. because they would require a disproportionate expenditure of time, cost and labour, leading to the risk of identification appearing de facto negligible.⁷³

Furthermore, the assessment of whether information qualifies as personal data must solely be based on objective criteria. Hence, the individual motivation or intention of actually identifying a natural person are irrelevant.

⁷² Kühling, Kühling/Buchner/Klar, “DS-GVO”, Art. 4 Nr. 1, Rec 21.

⁷³ CJEU judgment of 19 October 2016 – C-582/14 (“Breyer”).

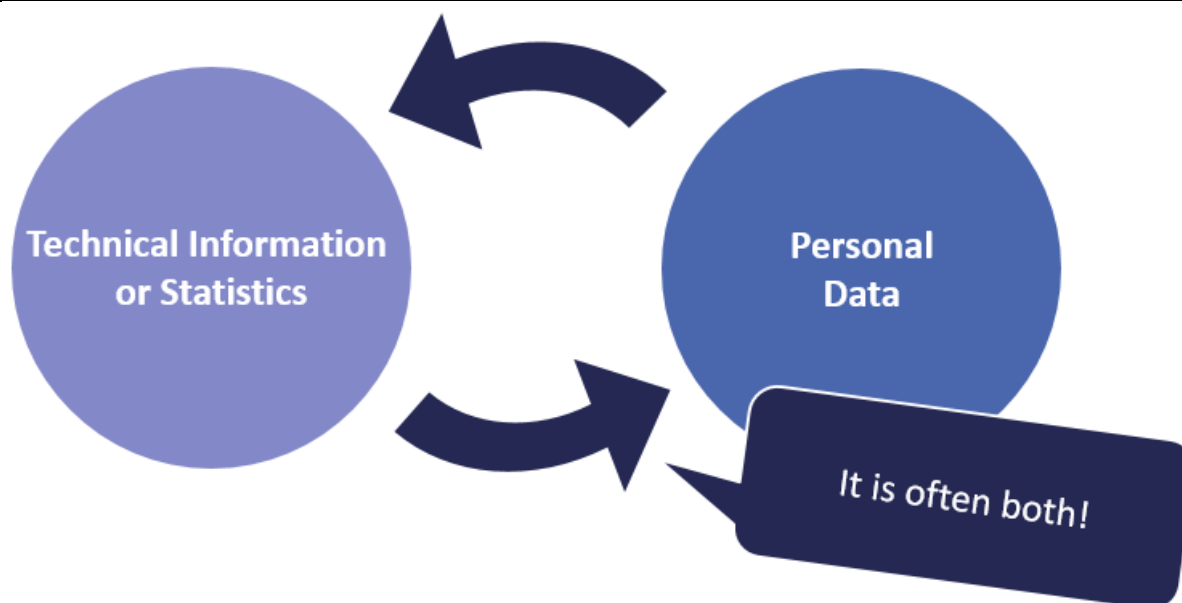


Figure 8 Interaction between technical Information / Statistics and Personal Data

In essence, as illustrated in the figure above, technical information can very often be allocated to an individual person, sometimes by means of using statistical information. Taking a closer look at the capabilities and means of allocating technical information to an individual person brings up the question, of whose knowledge, capabilities and means need to be considered in the assessment. In fact, the extent to which the knowledge, capabilities and means of third parties must also be taken into account has been the subject of a long-standing controversial dispute. In theory, as illustrated in the following figure, there are two opposing opinions characterised as an absolute and a relative approach.



Figure 9 Relative and absolute Approach of identifying a Natural Person

D4.1: Open Science in transport research: legal issues and fundamental principles

The problem concerns the question of whether the ability to establish a personal reference depends on the person responsible in the respective case (relative approach), or whether it is sufficient for any third party to be able to establish a personal reference (absolute approach). A number of hybrid forms can be found between the two extreme positions.⁷⁴

The CJEU tends to favour the relative approach, which became evident when it ruled that dynamic IP-addresses qualify as personal data even if only a third party, such as an internet service provider, has the necessary capabilities to identify the individual because this information is also likely to be used to identify the individual by other involved parties. Hence, these internet service providers were seen as a sufficient third party because their means of individualisation can under certain (not unlikely) circumstances be accessed by other parties.⁷⁵

Built on the CJEU conclusions, the guideline outlined in the following figure can help to determine whether information qualifies as personal data, which in turns is an important answer to the question of whether or not GDPR obligations apply.

⁷⁴ See for examples of such hybrid forms: Bergt, “Die Bestimmbarkeit als Grundproblem des Datenschutzrechts Überblick über den Theorienstreit und Lösungsvorschlag”, ZD 2015, 365 et seq.

⁷⁵ CJEU judgment 19 October 2016 – C-582/14, “Breyer”.

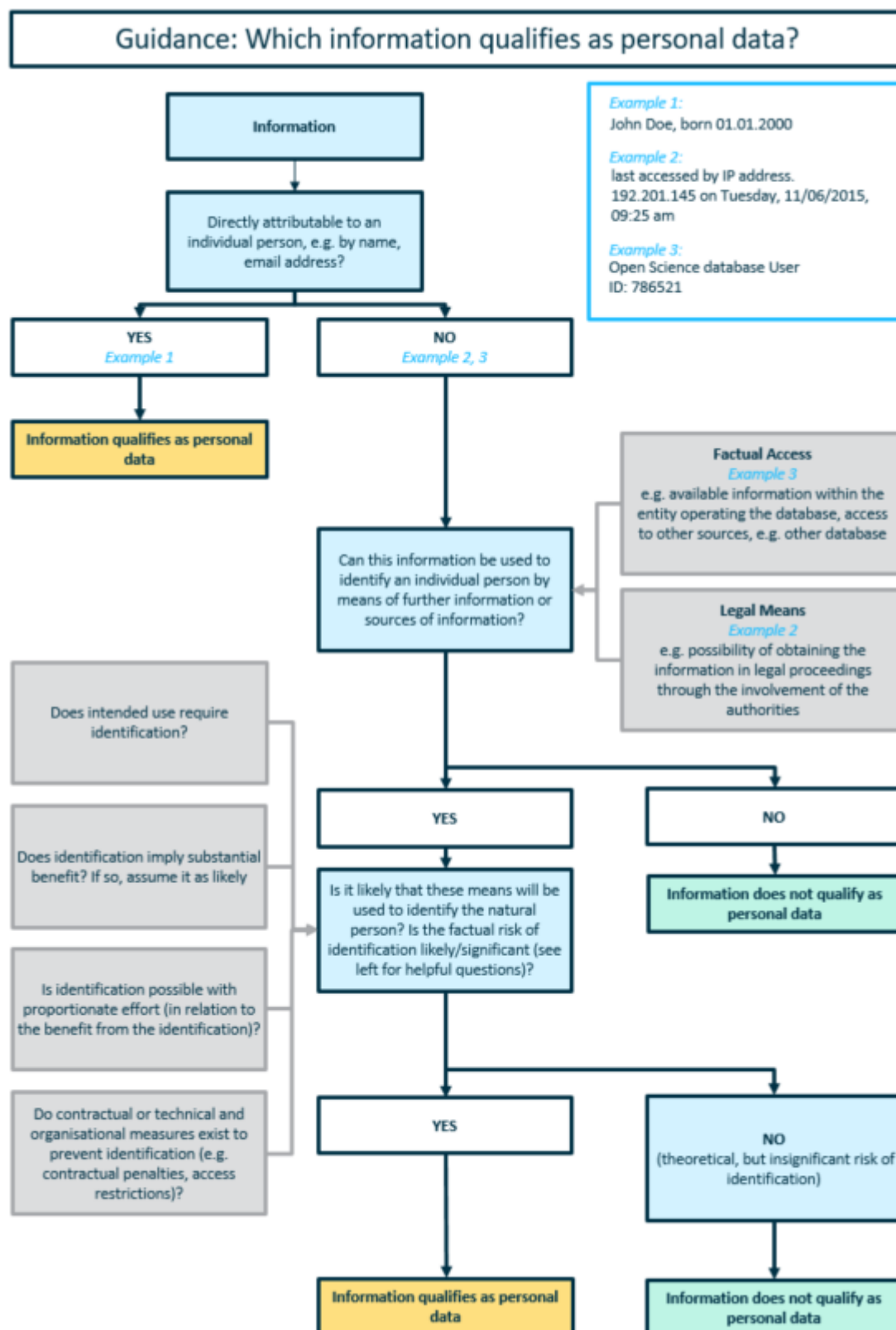


Figure 10 Guideline to qualifying Information as Personal Data

Types of Personal Data

Under the GDPR, all personal data are protected. Notwithstanding, the GDPR further distinguishes between ordinary and the more sensitive so-called special categories of personal data.⁷⁶ The processing of such special categories of personal data is subject to (even) stricter requirements. In particular, the processing of special categories of personal data is not eligible on bases of legitimate interests, thus removing the possibility of an otherwise very common legal bases for processing. Personal data qualifies as special category, where it reveals

- racial or ethnic origin,
- political opinions,
- religious or philosophical beliefs, or
- trade union membership,

and/or concerns

- genetic and/or biometric data for the purpose of uniquely identifying a natural person,
- health data, or
- data on a natural person's sex life or sexual orientation.

Such highly sensitive data is most likely not as commonly found in transport research as for example in the field of medical research. Notwithstanding, there are use cases of special categories of personal data in transport research as well, i.e. when assessing on handicapped accessible transportation or vehicle accident platforms holding references to injuries of individual persons.

Modalities of Data Processing covered by the GDPR

As a ground rule, essentially the GDPR applies to the following modalities as long as they are not merely carried out by a natural person in the course of a purely personal or household activity⁷⁷:

- Processing of personal data wholly or partly by automated means.
 - The term “automated” is not legally defined in the GDPR and is to be understood broadly, including all procedures in which at least part of a data processing activity is carried out automatically without further human intervention.
 - Digitisation of the processed data is a sufficient but not necessary condition for automation.

⁷⁶ Art 9 GDPR.

⁷⁷ Art 2 Para 2 lit c GDPR. Further exemptions are listed in Art 2 Para 2 – 4 GDPR; these are however not directly relevant to this deliverable.

D4.1: Open Science in transport research: legal issues and fundamental principles

- In any event, partial automation exists if a single data processing operation is partly manual and partly automatic. This is the case, for example, when personal data are manually entered into a digital database.
- In addition, partial automation can also be assumed if in several data processing operations, some of which are carried out manually and some of which are carried out automatically, are sufficiently closely linked to one another in a coherent processing operation.⁷⁸
- Non-automated processing of personal data, which form part of a filing system or are intended to form part of a filing system.⁷⁹
 - Since the concept of a filing system places only low demands on the structuring of the data contained therein, the GDPR covers practically all structured manual data collections.
 - Moreover, the GDPR is already applicable if the processed data are to be stored in a filing system some time along in the future.
 - As a result, largely only individual documents or unsorted collections of slips of paper do not fall within the scope of the GDPR as long as the structuring of this data is not intended.⁸⁰

In addition, the EU Member States legislators may extend the scope of application of the material GDPR application e.g. for processing of employee data by their employer.⁸¹

3.2.1.2 Territorial Scope of the GDPR

As briefly mention, contrary to popular belief, the GDPR does not only apply within the EU but may indirectly also apply far beyond the borders of the EU. The reason for this lies in the two principles determining the territorial scope in Art 3 GDPR containing of

- the principle of establishment⁸² and
- the marketplace principle⁸³ which requires further distinction in regards to
 - the supply of goods and services, and
 - the monitoring of behaviour of natural persons in the EU.

⁷⁸ Backer, Wolff/Brink, „BeckOK DatenschutzR DS-GVO“, Art. 2, Rec 1-5.

⁷⁹ Art 4 No 6 GDPR for the definition of a filing system.

⁸⁰ Backer, Wolff/Brink, „BeckOK DatenschutzR DS-GVO“, Art. 2, Rec 1-5.

⁸¹ Exemplary Sec 26 Para 7 Federal Data Protection Act (BDSG) for Germany.

⁸² Art 3 Para 1 GDPR.

⁸³ Art 3 Para 2 GDPR.

Furthermore, the GDPR also applies to the states of the European Economic Area (“EEA”). As such, Norway, Iceland and Liechtenstein have adopted the GDPR in July 2018. The following figure outlines the territorial scope.

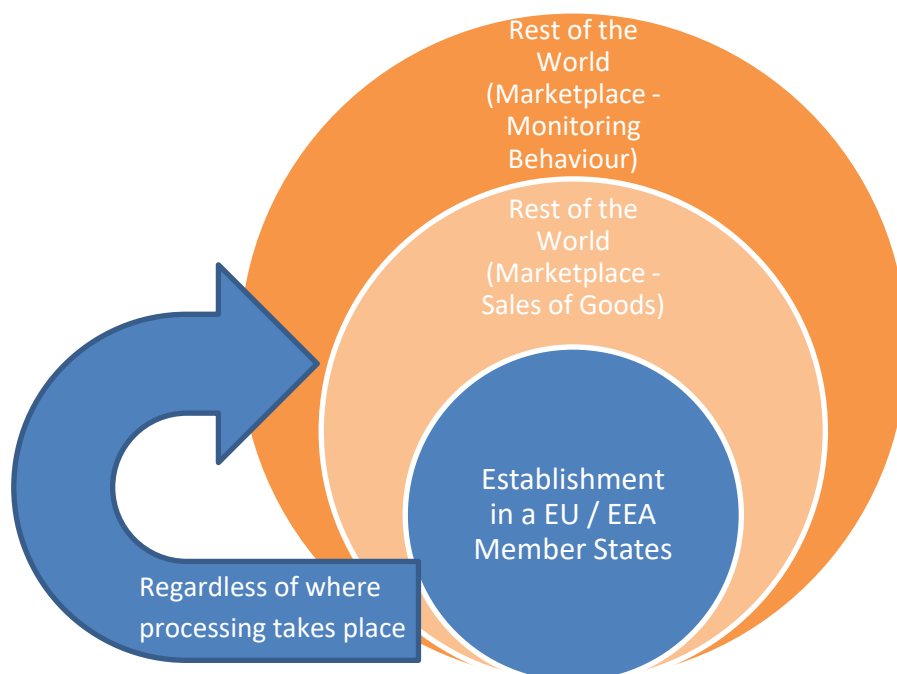


Figure 11 Territorial Scope of the GDPR

Principle of Establishment

Determining the territorial application of the GDPR on basis of the principle of establishment is usually not challenging and can easily be addressed when checking where the processing person or entity is established. If established in the EU / EEA, the GDPR always applies regardless of where in the world the processing ultimately takes place. This “establishment” implies the effective and real exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect.⁸⁴ Hence, the “establishment” does not need to be the primary office or a seat of the central administration.

Consequently, the place of establishment can also have an extraterritorial effect, leading to the territorial GDPR application for a data processing activity taking place outside the EU, which is however connected with an establishment in the EU. The determination of this “connection” can be difficult when dealing with several independent legal entities working together in a group-company structure. Here, the CJEU Google Spain decision showed that the court does not set high requirements on

⁸⁴ Rec 22 GDPR.

the element of connection, ruling that Google Spain is operating within the framework of the activities" of Google Inc. in the US.⁸⁵

Marketplace Principle

The marketplace principle explicitly extends the extraterritorial application of the GDPR to the rest of the world. Other than the aforementioned principle of establishment, the marketplace principle focusses on the destination of the processing activity, i.e. the place where the data subject is present during the processing. Most commonly, this applies to foreign companies involved in targeting customers in the European marketplace, offering their goods and services to natural persons in the EU. This e.g. is the case for a Chinese online marketplace offering goods directly to EU customers.

The second alternative of observing the behaviour is in practice far more relevant than one may think at first sight. The extra-territorial application of the GDPR is extended to monitoring the Internet activities of natural persons in the EU by non-EU persons or entities. This applies to common tracing of internet activities through device identifiers such as IP-addresses and cookie-IDs, which must first be assigned to a specific natural person in order to establish the personal reference.⁸⁶

This broad international application is aimed at reaching high privacy standards for individuals in the EU and binding people and entities involved in processing personal data within the EU to these high standards regardless of where the concerned data subject may be located.

3.2.2 Key Roles and Responsibilities under the GDPR

In terms of determining the key roles and responsibilities, the GDPR differentiates between controllers and processors. By definition, a controller is any person or entity that determines the purposes and means of the processing of personal data.⁸⁷ In contrast, a processor processes personal data on behalf of a controller.⁸⁸

3.2.2.1 Controller

By means of interpretation, the position of a controller is defined on a functional basis. The essential difference between a processor and a controller is that solely the controller determines the purposes and means of processing whereas the processor is bound by the controller's instructions.⁸⁹ To determine which person or entity factually determines and influences the processing of personal data, an analysis must show who decides about the "why" and the "how" of the processing of personal data along with related substantial questions essential to the lawfulness of processing. Turning towards the stakeholders in Open Science transport research, in principle individual persons are unlikely to qualify as controllers themselves. In fact, individual persons working as a research associate for a university or an employee for a company are bound to instructions based on their employment

⁸⁵ CJEU Judgment of 13 May 2014 – C-131/12 ("Google Spain"); also CJEU Judgement of 28 July 2016 – C-191/15 ("Amazon").

⁸⁶ *Hanloser, Wolff/Brink*, "BeckOK DatenschutzR DS-GVO", Art. 3 Rn. 37-41.

⁸⁷ Art 4 No 7 GDPR.

⁸⁸ Art 4 No 8 GDPR.

⁸⁹ *Klabunde, Ehmann/Selmayr*, "DS-GVO", Art. 4 Rn. 40; *Ingold, Sydow*, "Europäische Datenschutzgrundverordnung", Art. 4 Rn. 146.

D4.1: Open Science in transport research: legal issues and fundamental principles

contracts. As long as they process personal data within the boundaries of the instructions of their employer, their employer remains controller for all processing activities carried out by the research associate or employee.

3.2.2.2 Processor

On the contrary, the key element for the processor determination is the existence of instruction-based processing. An instruction means all kind of obligations transferred from the controller to the processor, i.e. through the underlying contract. Since instructions need to be explicit and sufficiently concrete, merely tolerating an action does not indicate an instruction.⁹⁰ However, data processing bound by instructions does not completely preclude the processor from making responsible decisions. Hence, the processor can still have a margin of judgement.⁹¹ In particular, the processor determination is not precluded by the fact that the processor may have higher expertise than its customer, giving him a certain amount of leeway for independent decisions. This may in particular apply to the delegation of the decision on the technical and organisational measures of data processing.⁹² In that case however, the framework in which the decisions can be made, is to be determined by the controller and the decision making scope is minor.⁹³ Furthermore, the controller in that case needs to monitor the processor's data processing.⁹⁴ Additionally, the controller needs to determine the subject matter and duration, the nature, means and purpose of the processing, the type of personal data and categories of data subjects.⁹⁵ Further distinguishing, with the permission of the controller, a processor is entitled to engage other processors, which are then commonly referred to as sub-processors.

3.2.2.3 Privacy Structures between multiple Controllers and/or Processors

An essential idea of Open Science is sharing information. Hence, it is inevitable that more than one stakeholder is involved in processing personal data in the field of Open Science in transport research. In fact, there is a complex interplay⁹⁶ between the obligations of

- the controller who is responsible for the processing of personal data,
- the person or entity responsible for the research which can often be a sponsor for the research, and

⁹⁰ *Spoerr*, Wolff/Brink, "BeckOK DatenschutzR DS-GVO", Art. 29, Rec 14; *Bertermann*, Ehmann/Selmayr, "DS-GVO", Art. 29, Rec 4; *Martini*, Paal/Pauly. "DS-GVO", Art. 29, Rec 18.

⁹¹ *Spoerr*, Wolff/Brink, "BeckOK DatenschutzR DS-GVO", Art. 28, Rec 27; Art. 29, Rec 8.

⁹² Gola, "Aus den aktuellen Berichten und Informationen der Aufsichtsbehörden (40): Offene Fragen bei der Beschäftigtendatenverarbeitung: Gehaltsabrechnung durch Steuerberater und Verarbeitungen beim Betriebsrat", RDV 2019, 73.

⁹³ *Bertermann*, Ehmann/Selmayr, "DS-GVO", Art. 28 Rec 3, *Hartung*, Kühling/Buchner, "DS-GVO", Art. 28 Rec 47.

⁹⁴ *Hartung*, Kühling/Buchner, "DS-GVO", Art. 28 Rec 48.

⁹⁵ *Spoerr*, Wolff/Brink, "BeckOK DatenschutzR DS-GVO", Art. 29, Rec 8.

⁹⁶ See European Data Protection Supervisor, "A Preliminary Opinion on data protection and scientific research", P 6, edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf, last accessed 14 August 2020.


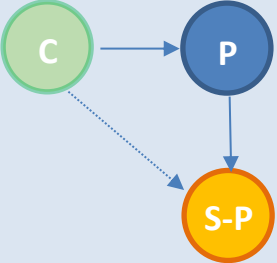
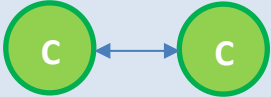
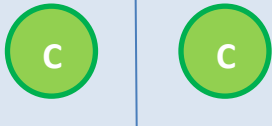
D4.1: Open Science in transport research: legal issues and fundamental principles

- the actual researcher who is involved in carrying out the actual research, who can depending on the circumstances be a separate controller, joint controller and/or processor.

In broad terms, on the one hand, other actors can merely be involved as processors or even sub-processors if they do not determine the means and purposes of data processing. The more likely case however is, that numerous actors shall participate in Open Science activities for their own purposes, which obviously also can be shared or joint purposes.

When more than one actor is involved in the processing of personal data, the structure between the involved actors needs to be analysed. In most cases, the involvement of more than one actor in processing activities triggers mandatory obligations under the GDPR, including mandatory contractual structures and information obligations. An overview can be found in the following table:

Table 2 Overview on Privacy Structures between multiple Controllers and/or Processors

Controller-Processor Structure	Processor-Sub-Processor Structure	Joint Controller Structure	Individual Controller Structure
			
<p>The Controller determines the means and purposes of data processing.</p> <p>The Processor processes data on behalf of the Controller.</p>	<p>The Processor engages a Sub-Processor with the permission of the Controller.</p> <p>Both, Processor and Sub-Processor do not determine means and purposes of the data processing and process data on behalf of the Controller.</p>	<p>Two Controllers jointly determine the means and purposes of data processing in regards to the same data subjects.</p>	<p>Two Controllers interact but individually determine the means and purposes of data processing.</p>
<p>Art 28 GDPR</p> <p>The GDPR requires the conclusion of a data processing agreement consisting of the criteria listed in Art 28 GDPR.</p>	<p>Art 28 Para 2, 4 GDPR</p> <p>The GDPR requires Sub-Processors to also be bound to a data processing agreement consisting of the same obligations between the Controller and the Processor.</p>	<p>Art 26 GDPR</p> <p>The GDPR requires Joint Controllers to conclude an arrangement and inform the data subjects of the essential content of the agreement. The GDPR does not list detailed mandatory elements for the agreement and rather</p>	<p>Art 24 GDPR</p> <p>In relation to each other, individual Controllers are generally not obliged to conclude any sort of agreement. There are however contractual structures e.g. to safeguard international data transfers in cases where an EU-based</p>

D4.1: Open Science in transport research: legal issues and fundamental principles

		broadly describes that the agreement needs to transparently determine the respective responsibilities for compliance with the obligations under the GDPR.	Controller wants to share data with a non-EU-based other individual Controller.
--	--	---	---

3.2.3 Data Protection Principles

The GDPR holds six overarching data protection principles, which must be observed in all processing of personal data at any time. They are closely connected to the essential elements of the right to the protection of personal data under the EU Charter of Fundamental Rights (“EU CFR”).⁹⁷ As the following assessment will show, all six data protection principles affect every aspect of Open Science in transport research within the scope of the GDPR. In addition to these mandatory principles, the GDPR requires controllers to keep and maintain sufficient documentation to prove compliance with the data processing principles.

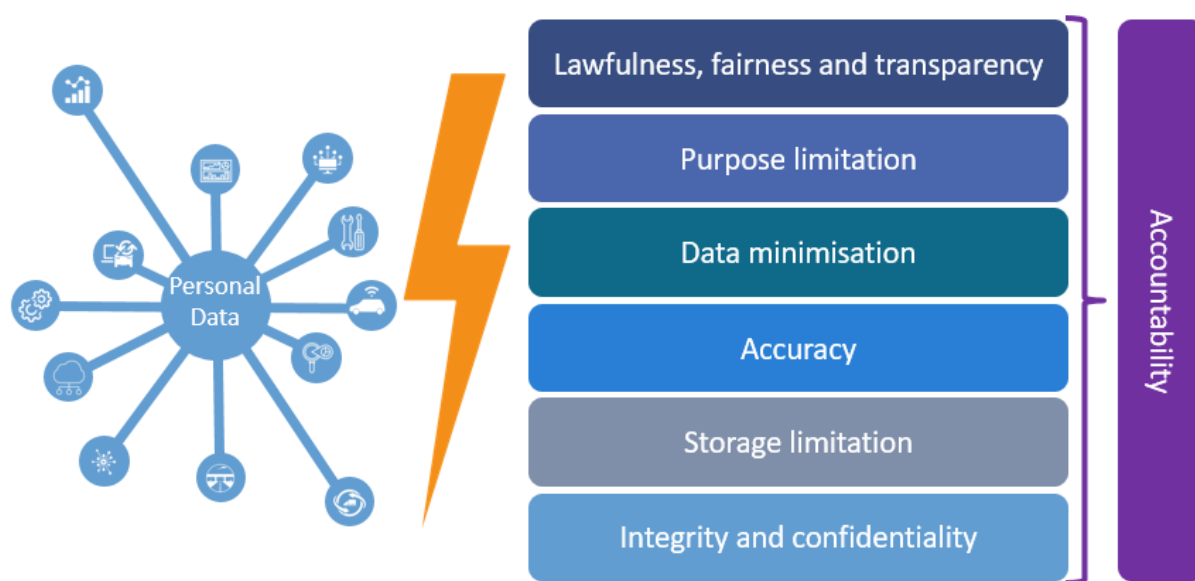


Figure 12 GDPR essential Data Processing Principles

3.2.3.1 Lawfulness, Fairness and Transparency

The first set of basic principles is defined in Art 5 Para 1 lit a GDPR. Although the three principles included in the set have mutual substantive references to each other, they are not necessarily linked. Essentially, as an overarching principle, all processing of personal data must be:

- based on a valid legal basis, as mentioned above (“lawful”);

⁹⁷ Art 8 Para 2 Charter of Fundamental Rights of the European Union.

D4.1: Open Science in transport research: legal issues and fundamental principles

- the interests and expectations of data subject shall always be taken into account and never be ignored. The data subjects' trust may never be exploited e.g. through misconceptions ("*fair*")⁹⁸;
- data subjects must always be duly informed about the processing of their personal data in an easily accessible manner, written in plain, intelligible and simple language ("*transparent*")⁹⁹.

3.2.3.2 Purpose Limitation

The mandatory purpose limitation of processed data is legally defined in Art 5 Para 1 lit b GDPR. In principle, all personal data may only be collected and further processed for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

This means that apart from the initial collection of the personal data, any secondary use also requires a legal basis and all secondary purposes may not be incompatible with the initial purpose. There is however a reference to an opening clause for scientific research purposes; this will be discussed in Sec 3.2.5. To prevent any circumvention of this important basic principle, the original purpose must be interpreted narrowly.¹⁰⁰ Hence, general and unspecified initial purposes for the data collection are no viable option to create a legal basis for secondary use.

3.2.3.3 Data Minimisation

The mandatory data minimisation of processed data is legally defined in Art 5 Para 1 lit c GDPR. In principle, all personal data may only be processed to an extent that is adequate, relevant and limited to what is necessary in relation to the legitimate purposes for which they are processed.

Consequently, the type, scope and duration of processing must be limited, at best using means of technological design (privacy-by-design)¹⁰¹ Furthermore, data protection-friendly default settings must always be chosen (privacy-by-default).¹⁰² Here, there is a strong overlap to mandatory privacy related security aspects, which are discussed in Sec 3.4.1 of this document.

3.2.3.4 Accuracy

The mandatory principle of accuracy is legally defined in Art 5 Para 1 lit d GDPR. In principle, all personal data needs to always be accurate and, where necessary, kept up to date and every reasonable step must be taken to ensure that inaccurate personal data are erased or rectified without delay.

In addition to the aforementioned principle of data minimisation, the principle of accuracy also requires that incorrect data be deleted or corrected immediately. This leads to enormous practical significance because the processing of existing data is not completed and creates obligations for as long as the data are still available.

⁹⁸ Schantz, Wolff/Brink, "BeckOK DatenschutzR DS-GVO", Art. 5, Rec 7-9.

⁹⁹ Ibid, Rec 10, 11.

¹⁰⁰ See based on former Directive 95/46/EC ("**Data Protection Directive**"): Art 29 Data Protection Working Party, "Opinion 03/2013 on purpose limitation", WP 203, P 16.

¹⁰¹ Art 25 Para 1 GDPR.

¹⁰² Art 25 Para 2 GDPR.

3.2.3.5 Storage Limitation

The mandatory principle of storage limitation is legally defined in Art 5 Para 1 lit e GDPR. In principle, all personal data must be kept in a form permitting identification of data subjects for no longer than necessary for the purposes for which the personal data are processed.

Furthermore, there is a reference to an opening clause for scientific research purposes, which again will be discussed in Sec 3.2.5 and is subject to the implementation of the appropriate technical and organisational measures, which in turns are discussed in Sec 3.4.1 of this document.

The storage limitation is a key requirement to safeguard the rights and freedoms of the data subject. It shows, that all processing of personal data has an expiration date leading to the obligation of regularly assessing the current achievement of processing purposes in relation to the interests of the data subject in order to be allowed to continue storing the data.¹⁰³

3.2.3.6 Integrity and Confidentiality

The mandatory principles of integrity and confidentiality storage limitation are legally defined in Art 5 Para 1 lit f GDPR. In principle, all personal data may only be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Hence, again, there is a strong overlap to mandatory privacy related security aspects, which are discussed in Sec 3.4.1 of this document. In essence, all processing of personal data requires efficient technological and technical measures for protection against unauthorised access and processing by third parties ("*confidentiality*"), for example by encrypting personal data as well as freedom from any manipulation of data (*integrity*).¹⁰⁴

3.2.4 Legal Basis for processing Personal Data

Following the aforementioned principle of lawfulness, all processing of personal data requires a legal basis. The GDPR lists six different legal bases¹⁰⁵, of which at least one must apply to any data processing activity.

Regarding these legal bases listed in the GDPR, in context of Open Science in transport research, there are only four plausible legal bases for processing of personal data:

- Freely given, explicit consent of the data subject.
- Necessity for the performance of a contract to which the data subject is a party (including prior steps to entering into the contract).
- Compliance with a legal obligation to which the controller is subject.

¹⁰³ CJEU Judgment of 13 May 2014 – C-131/12 ("Google Spain").

¹⁰⁴ CJEU Judgment of 8 April 2014 – C-293/12 and C-594/12 ("Digital Rights Ireland").

¹⁰⁵ Art 6 Para 1 GDPR.

D4.1: Open Science in transport research: legal issues and fundamental principles

- Necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where overridden by interests or fundamental rights and freedoms of the data subject.

The following figure highlights these relevant legal bases within the scope of Art 6 Para 1 GDPR for the processing of personal data.

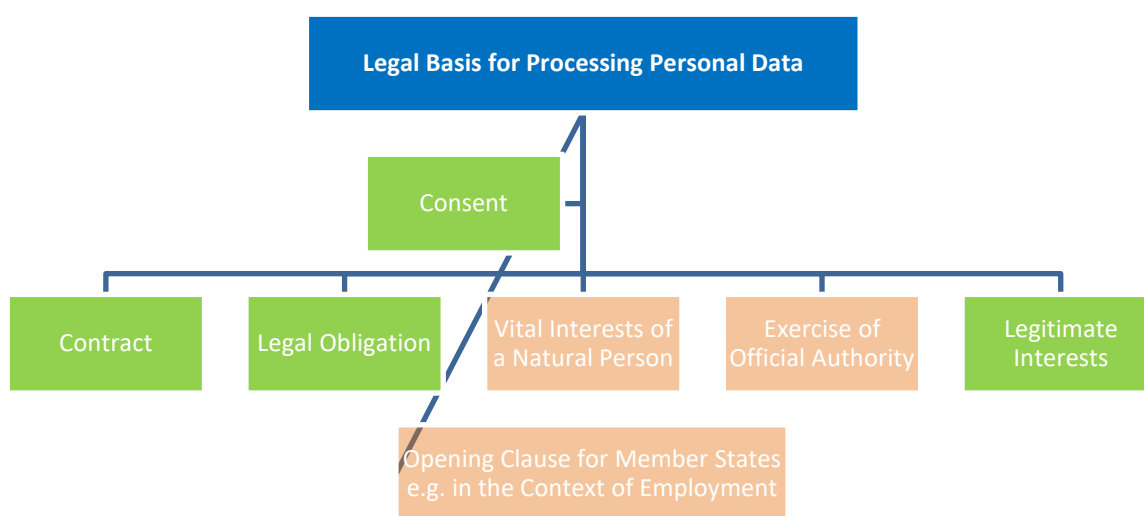


Figure 13 Overview on legal Bases for processing Personal Data

Apart from the set of legal bases listed explicitly in the GDPR, the GDPR contains opening clauses allowing EU Member States to substantiate the legal bases under national law. Most EU Member States have made use of the opening clauses e.g. in an employment context. However, all opening clauses in relation to the legal basis do not allow the EU Member States to introduce entirely new sets of legal bases. The employment context under German Member State law is a good example here to illustrate: Employees are bound to their employer by means of a contract. In order to fulfil this contract, the employer needs to process personal data of the employee. Furthermore, the employer is subject to legal obligations in terms of the employment relationship, such as paying mandatory employer social security contributions directly to the authorities. Hence, under the GDPR, these processing activities would be covered partly under the contract and partly under the legal obligations. Here, the German legislator made use of the opening clause in Art 88 GDPR and introduced a national legal basis covering all necessary data processing in an employment relationship.¹⁰⁶ Materially however, this does not lead to a deviation of the legal bases in regards to the GDPR.

Hence, in the context of Open Science in transport research, these deviations in EU Member State Laws are legally not relevant. On a related note, essential deviations between the EU Member States'

¹⁰⁶ Sec 26 German Federal Data Protection Act (BDSG).

laws need to be avoided in the context of Open Science anyways, because these borders are contrary to the essential ideals of Open Science.

3.2.4.1 Consent

Consent means that the data subject has explicitly provided an affirmative action, indicating permission to process its personal data for one or more specific purposes. Consent must be freely-given and be specific, informed and unambiguous.

Essentially, the notion of the explicit purpose is key here. The data subject needs to know who exactly will process data for which exact purposes. Furthermore, the data subject must provide consent freely, without any form of undue pressure. Consent may neither be bundled-up as a non-negotiable part of terms and conditions, nor with the provision of a contract of a service for which these personal data are not necessary. If such bundling occurs, the declaration of consent will in turns be presumed to not have been freely given.¹⁰⁷

Furthermore, the EDPB is particularly strict about the concept of granular consent and states that consent of the data subject should be given in relation to one or more specific purposes and the data subject should have a real choice in relation to each of them.¹⁰⁸ Notwithstanding, services may involve multiple processing operations for more than one purpose. It concludes that in such cases, the data subjects should be free to choose which purpose they accept, rather than having to consent to a bundle of processing purposes. In a given case, several declarations of consent may be warranted to start offering a service, pursuant to the GDPR. This is stated against the essence of Recital 43 GDPR which clarifies that consent is presumed not to be freely given if the process/procedure for obtaining consent does not allow data subjects to give separate consent for personal data processing operations respectively (e.g. only for some processing operations and not for others) despite it being appropriate in the individual case.

However, this concept of granularity does not pose a serious legal barrier for Open Science in transport research as long as the Open Science processing purposes form a coherent generic term for the allocated processing purposes under it. This is underlined by Recital 32 GDPR, which states that consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them.

The main legal barrier for consent as legal basis for processing data in an Open Science context is the fact that by definition, Open Science is aimed at an unlimited group of people. Also, pursuant to BE Open deliverable D 1.1¹⁰⁹, the stakeholders and their characterisation is broad and far reaching, including

- research centres and universities,
- researchers and students,

¹⁰⁷ European Data Protection Board, “Guidelines 05/2020 on consent under Regulation 2016/679”, Version 1.1, P 7 et seq., edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf, last accessed 14 August 2020.

¹⁰⁸ Ibid, P 13 et seq.

¹⁰⁹ BE OPEN deliverable D 1.1, “Taxonomy of actors, terminology and experimental tools”, P 26.

- private researchers,
- policy makers (regional, national and international level),
- transport networks,
- NGOs and community organisations,
- commercial transport and logistics industry players, and
- interested citizens.

Taking into account the variety of stakeholders and the different purposes they aim to achieve by means of processing personal data, it becomes evident that consent comes with a high risk of being invalid and should thus serve as last resort when determining a legal basis for the processing of personal data.

On a related note, it is not advisable to gather consent in addition to another legal basis of processing against the background that the data subject must be able to withdraw its consent at any time. Although the wording of Art 6 Para 1 Sentence 1 GDPR clearly suggests that there can be more than one legal basis¹¹⁰, including consent, this is often disputed. Critics of the literal interpretation argue that the concept of consent relies on giving the data subject the free choice of whether or not personal data shall be processed. If on the contrary, processing were to still remain valid on another legal basis after the data subject decided to withdraw consent, then it can be argued that consent was not freely given in the first place.¹¹¹

3.2.4.2 Contract

Processing of personal data can be based on a contract, if it is necessary for the fulfilment of the contract and the data subject freely entered into this contract as a party. The wording "*performance of a contract*" in Art 6 Para 1 lit b GDPR indicates that for the contract to apply as a legal basis, it is not necessary that the contractual partner of the data subject and the controller are identical. Rather, the wording requires only that the data subject is a party to the contract.¹¹² This understanding of the law widens the scope for this legal basis by covering uninvolved third parties if this is necessary for the performance of a contract to which the data subject is a party to.

In an Open Science in transport research context, a contract can potentially serve as legal basis for instance, where a publishing data subject has a contract with a university to provide research or with a platform to publish research.

3.2.4.3 Legal Obligation

Legal obligations are an important legal basis for the processing of personal data.¹¹³ This legal basis aims at harmonising the legal system both on a national level and on a EU Member State level. It is

¹¹⁰ The GDPR reads (underlined by author): "Processing shall be lawful only if and to the extent that at least one of the following applies: (...)".

¹¹¹ Buchner/Petri, Kühling/Buchner, "DS-GVO" Art. 6, Rec 22-24.

¹¹² Albers/Veit, Wolff/Brink, "BeckOK DatenschutzR DS-GVO", Art. 6, Rec 30.

¹¹³ Art 6 Para 1 lit c GDPR.

D4.1: Open Science in transport research: legal issues and fundamental principles

important to keep in mind that “legal obligation” does not cover any contractual obligations based on an autonomous private decision but rather requires an obligation by virtue of the laws of the EU or of a EU Member State.¹¹⁴ Hence, since legal obligations of countries outside the EU are not covered, this leads to practical issues on an international level, e.g. when a database is hosted in the United States of America (“US”) and US-law requires the processing of personal data. The legal basis for such processing must then be found somewhere else, usually in legitimate interests.¹¹⁵

In context of Open Science in transport research, the various respective laws of the EU Member States contain a wide variety of legal obligations. This however will usually not help to constitute a legal basis for all transport research related processing activities, since all processing activities necessary to fulfil a legal obligation are as such strictly conditional to the sole purpose of fulfilling this respective legal obligation. Exemplary, in transport research there can be a legal obligation from an IPR perspective to mention the author of an academic publication, which in turns requires the processing of this author’s name.

In essence, legal obligations as legal basis requires:

- the processing of personal data is necessary to comply with a common law or statutory obligation of a EU Member State, which does not include contractual obligations,
- the processing must be strictly necessary in order to fulfil the legal basis, and
- the legal basis should be clearly identified and the assessment of necessary processing activities under the legal obligation must be duly documented.

3.2.4.4 *Legitimate Interests*

Where personal data inevitably need to be processed, the principles for Open Science in transport research can best be achieved by a preferably broad legal basis for the processing of personal data. This preferably broad scope of a GDPR legal basis can be found in legitimate interests pursuant to Art 6 Para 1 lit f GDPR.

The legal basis of legitimate interests widens the scope in comparison to the other legal bases in the GDPR because unlike any other legal basis, it is neither centred on a particular purpose (such as performing a contract with the individual or complying with a legal obligation), nor limited to processing that the individual has specifically agreed to (consent).

Hence, benefitting Open Science in transport research, legitimate interests are more flexible and can generally apply to any type of processing for any reasonable purpose within the boundaries of the law.¹¹⁶

¹¹⁴ Albers/Veit, Wolff/Brink, “BeckOK DatenschutzR DS-GVO”, Art. 6, Rec 34,35.

¹¹⁵ Sec 3.2.5 for further information on safeguards for international data transfers.

¹¹⁶ It is important to keep in mind that sensitive categories of personal data cannot be processed on basis of legitimate interests.

D4.1: Open Science in transport research: legal issues and fundamental principles

The key challenge for controllers lies in the onus of balancing the interests and assessing the necessity of the processing activity in light of overriding interests of the data subjects. The key elements of the legitimate interest provision can be broken down into a three-part test.¹¹⁷

- Purpose Test – is there a legitimate interest behind the processing?
- Necessity Test – is the processing necessary for that purpose?
- Balancing Test – is the legitimate interest overridden by the individual's interests, rights or freedoms?

In essence, all abovementioned test-aspects must be fulfilled and documented prior to commencing with the processing activity.

Purpose Test

Determining a legitimate interest is rarely challenging, since the term is very broad and includes the legitimate interests of any third party or even the general public. This can be important for Open Science in transport research to the extent that research is seen as benefit to society, which in turns adds weight to the interests when balancing them against those of the individual in step three of the test.

Since legitimate interest must always be documented, it is not sufficient to rely on vague or generic interests somewhere in the future.

Necessity Test

The necessity test is closely connected with the aforementioned principle of data minimisation (see Sec 3.2.3.3). In this part of the test, the controller needs to assess and document, that the respective processing activity is necessary for the purposes of the determined legitimate interests in step one. This necessity does not need to qualify as absolutely conditional; it is sufficient if the processing is a targeted and proportionate way of achieving the purpose. The challenging aspect in this step of the test is deciding whether the processing is proportionate and adequately targeted to meet the pre-determined objectives, and whether there is any less intrusive alternative. This would be the case if the purpose can be achieved with less personal data, less invasive processing activities or even without personal data.

Balancing Test

The essential part of the test lies in balancing the interests of the involved stakeholders. The most challenging aspect usually is properly determining the potential impact of the processing on individual data subjects. These impacts can be simple interests, or even fundamental rights and freedoms of

¹¹⁷ Information Commissioner's Office – ICO, "What is the legitimate interests' basis?", ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/what-is-the-legitimate-interests-basis/#:~:text=Legitimate%20interests%20is%20one%20of,%2C%20fairness%20and%20transparency'%20principle, last accessed 14 August 2020.

the data subject. Recital 75 GDPR provides more concrete guidelines for determining risks to individuals' rights and freedoms by listing physical, financial or any other impact, such as:

- the inability to exercise individual rights (including data protection rights);
- loss of control over the use of personal data; or
- any social or economic disadvantage.

Having determined the potential impact for the data subject, this impact needs to then be balanced against the determined interests in step one. This balancing is significantly influenced by the reasonable expectation of the data subject, which is clearly linked to transparency obligations of the controller.¹¹⁸ Since these transparency obligations are mandatory, they can only negatively influence the balancing of interests. It is a matter of course that the data subject is put into a position to exercise its rights, without this being a fact that can positively influence the balancing of interests.¹¹⁹

In essence, for the balancing of interests, the objective assessment of whether the individual can reasonably expect the processing is key, taking into account in particular when and how the data was collected.

3.2.5 Privilege for scientific Research

The GDPR holds a variety of opening clauses, allowing EU Member States to lower the burden of privacy obligations under the GDPR for scientific research. As such, the GDPR acknowledges that scientific research depends on the exchange of ideas, knowledge and information and cannot generally exclude that any of this information contains personal data. The GDPR also acknowledges that research benefits the society and therefore allows for the presumption of compatibility in regards to the processing of data collected in commercial and other context for scientific research purposes. Furthermore, there is a general assumption that research occurs within a framework of ethical oversight, which in turn leads to responsible risk management.¹²⁰ As such, the fundamental principles of research integrity assessed in Sec 4.2 constitute an important element of such a framework.

3.2.5.1 Definition of scientific Research

Although referring to scientific research in 13 occasions, the GDPR does not hold a definition to explain the scope of research application. Furthermore, there is no universally agreed definition of "scientific research" or even "research". Commonly, definitions of research tend to focus on systematic activity, which includes the gathering and further analysis of data, increasing the level of understanding and knowledge as well as their application.¹²¹

¹¹⁸ The most important transparency obligations can be found in the mandatory information pursuant to Art 13, 14 GDPR.

¹¹⁹ Recital 47 GDPR for further information.

¹²⁰ European Data Protection Supervisor, A Preliminary Opinion on data protection and scientific research, P 2, edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf, last accessed 14 August 2020.

¹²¹ OECD Glossary of Statistical Terms, stats.oecd.org/glossary/detail.asp?ID=2206, last accessed 14 August 2020, Bartolotti/Heinrichs, "Delimiting the concept of research: an ethical perspective".

D4.1: Open Science in transport research: legal issues and fundamental principles

The definition of scientific research adds scientific methods of conducting research as criterion, which predominantly builds on the principle of an open dialogue of validating the achieved hypothesis and conclusions to distinguish between science and pseudo-science. As for the involved fields of research, there is no distinction between natural sciences and human sciences as well as also not between commercially influenced research and non-profit research.¹²²

Hence, the GDPR requires a broad interpretation of scientific research covering any independent and autonomous intellectual activity with the aim of acquiring new knowledge in a methodical, systematic and verifiable manner.

3.2.5.2 Scope of GDPR deviations for scientific Research

The privilege for scientific research under the GDPR mainly consists of specific opening clauses allowing for derogations from certain controller obligations and an accompanying provision on appropriate safeguards.¹²³ Through these opening clauses, the GDPR allows the EU Member States to adapt privacy obligations to the specific circumstances and public interests served by scientific research activities. At the same time, the GDPR clearly points out, that scientific research activities can never be grounds to fall out of the scope of the GDPR application. Through the research privilege, a fair balance between individual rights of data subjects and other interests in the society is to be reached.

However, the privileges of scientific research are bound to the assumption that scientific research is beneficial to the whole of society and that scientific knowledge is a public good to be encouraged and supported. Hence, performing an activity deemed research does not provide a sufficient basis for taking irresponsible risks because the principles of lawfulness, fairness and transparency remain untouched. Furthermore, simply claiming to process data for the purposes of scientific research is not sufficient and coherence to sector-related methodological and ethical standards is partly argued to be conditional groundwork in order to rely on the privileges for scientific research under the GDPR.¹²⁴ Overall, privileges for scientific research cannot be applied in such a way that the essence of the right to data protection is undermined because any limitation to fundamental rights must be interpreted restrictively.¹²⁵ In particular, excessive application might be considered abusive for instance in light of applying indefinite retention periods for personal data and denying data subjects rights to information.

In conclusion, the GDPR does not provide comprehensive privilege for scientific research purposes but rather follows the approach of enabling privileges in regards to certain aspects of the controller obligations. Furthermore, although most EU Member States have adopted privileges for scientific research, the fact that research privileges do not apply directly but rather by ways of opening clauses lead to a landscape of (slightly) different material laws in EU Member States which in turns poses a challenge for the borderless Open Science in transport research approach. Notwithstanding, the

¹²² Herbst, Kühling/Buchner, “DS-GVO”, Art. 5 Rn. 53.

¹²³ Art 89 Para 1 GDPR.

¹²⁴ European Data Protection Supervisor, A Preliminary Opinion on data protection and scientific research, edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf, last accessed 14 August 2020.

¹²⁵ i.e. CJEU Judgment of 8 April 2014 – C-293/12 and C-594/12 (“Digital Rights Ireland”).

D4.1: Open Science in transport research: legal issues and fundamental principles

mere acceptance of importance of scientific research may be valued in determining a legal basis for the processing of personal data, in particular in terms of legitimate interests.¹²⁶

An overview on the material scope of opening clauses for scientific research purposes can be found in the following table:

Table 3 Overview on Privilege for scientific Purposes under the GDPR

Definition of scientific Purposes	Addressee	Opening Clauses
<p>No definition in the GDPR</p> <ul style="list-style-type: none"> • Rec 159 GDPR: Scientific research purposes • To be interpreted broadly, incl. <ul style="list-style-type: none"> ○ technological development ○ demonstration ○ fundamental research ○ applied research ○ privately funded research <p>Scientific Research is commonly understood as:</p> <p><i>Independent and autonomous intellectual activity with the aim of acquiring new knowledge in a methodical, systematic and verifiable manner.</i></p>	<p>Anyone who</p> <ul style="list-style-type: none"> • independently researches • according to scientific methods • for the purpose of acquiring knowledge 	<p>Allow national exceptions, e.g.</p> <ul style="list-style-type: none"> • Art 85 Para 2 GDPR (comprehensive exceptions for academic expression) • Art 89 Para 2 GDPR (data subjects rights) • Art 5 Para 1 lit b, e GDPR (purpose and storage limitation) • Art. 9 Para 2 lit j GDPR (special categories of data) • Art 14 Para 5 lit b GDPR (Information) • Art 21 Para 6 GDPR (right to object)

3.2.6 Safeguards for international Data Transfer

Open Science in transport research is not supposed to experience any borders. Notwithstanding, to the extent that Open Science requires the processing of personal data within the scope of the GDPR, there are significant legal obligations that need to be followed. The GDPR is based on the idea that within the EU and EEA, the harmonisation of the privacy laws through the GDPR leads to an equal level of protection. As soon as personal data now leaves this safe region, additional mandatory safeguards apply. Pursuant to Chapter 5 GDPR, the most essential safeguards for data transfer are:

- EU Commission adequacy decisions based on Art 45 GDPR.
- EU Commission approved Standard Contractual Clauses ("SCC") based on Art 46 GDPR.

The existing SCC are a popular and cost-efficient mechanism to safeguard international data transfers on a contractual basis. They consist of (currently) three pre-drafted contracts which may not be amended by the parties accept for filling in the required information asked in the contracts.¹²⁷ From an Open Science in transport research perspective, the use of standard contractual clauses can be

¹²⁶ See Sec 3.2.4.4 on legitimate interests as legal basis.

¹²⁷ See for further information on the existing SCC, ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en, last accessed 14 August 2020.

D4.1: Open Science in transport research: legal issues and fundamental principles

detrimental because they would require adding a contractual layer to all possible international data transfers.

Here, the adequacy decision can provide an easier solution. Where a valid adequacy decision exists and there is a legal basis for the processing, personal data can flow from the EU and to third countries without any further safeguards. Essentially, data transfers to such a safe country are treated similarly to transfer of data within the EU. So far, the EU Commission has recognised an adequate level of security in the following countries¹²⁸:

- Andorra,
- Argentina,
- Canada (for commercial organisations),
- Faroe Islands,
- Guernsey,
- Israel, Isle of Man,
- Japan,
- Jersey,
- New Zealand,
- Switzerland and
- Uruguay.

Furthermore, and this is very important from a practical point of view, the EU Commission had accepted a (self-)certification mechanism for the US, called “EU-US-Privacy-Shield” as adequate.

In an earthquake-like decision, the CJEU has invalidated the EU-US-Privacy-Shield in its judgement of 16 July 2020 in case C-311/19. Additionally, the court has put up additional burdens on the use of the SCC. In essence,

- The CJEU invalidated the EU-US-Privacy-Shield with immediate effect. Thus, the transfer of data from the EU to a data recipient in the US currently rendered on basis of a respective EU-US Privacy Shield certification of the data recipient is unlawful and must therefore be suspended or shifted over to another transfer mechanism envisaged by Chapter 5 GDPR.
- SCC generally remain a valid mechanism to transfer personal data outside of the EU. This generally may also still apply to data transfers to the US. Accordingly, as a first line of de-

¹²⁸ See the EU Commission website on adequacy decisions for more information, ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en, last accessed 14 August 2020.

fence, it generally remains an option to replace the Privacy Shield guarantees by SCC. Yet, the use of SCC is subject to an individual positive risk assessment to be rendered by the data exporter.

- Data exporters must on a case-by-case basis consider whether the data importer located outside of the EU is capable of complying with its obligations stemming from the SCC. Insofar, the SCC require that the respective processing is carried out in accordance with the applicable data protection laws of the data exporter (hence the GDPR). To this end, data exporters must evaluate whether the relevant legal regime to which the data importer is subject may interfere with this obligation or – framed in a more positive manner – (in conjunction with the SCC) provides for a level of protection (for data subjects) essentially equivalent to that guaranteed within the EU by the GDPR read in the light of the EU CFR.
- If the data exporters do not live up to their respective obligations, the data protection supervisory authorities are called to suspend or prohibit any data transfer outside of the EU in case they deem that a data recipient (due to its local legal regime) does not or cannot comply with its obligations stemming from the SCC and the protection of the data transferred cannot be ensured by other means.

To which extent changes result from this CJEU decision which materially affect Open Science in transport research is too early to say and must duly be monitored throughout time. Notwithstanding, it must be taken into account, that many digital service providers along with state-of-the-art software manufacturers involved in the processing of personal data are located in the US.

3.2.7 Anonymisation

The GDPR does not provide a definition for anonymisation but rather only focusses on providing a definition for pseudonymisation – these terms however are not equivalent.¹²⁹ Essentially, anonymisation is the process of creating anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.¹³⁰ Hence, anonymisation is an improvement over pseudonymisation, where the use of additional, but separately stored information is sufficient for identification.

Since the GDPR is not applicable to anonymous data pursuant to Rec 26 GDPR, working with anonymous data avoids all legal privacy issues. In many cases, information can be put to good use without it being necessary to know to whom it relates. In these cases, it is advisable to avoid or remove the personal reference. On the one hand, this protects the data subjects and on the other hand, it spares the data controller the applicability of data protection law with all detrimental effects of being

¹²⁹ Art 4 No 5 GDPR.

¹³⁰ Ziebarth, Sydow, “Europäische Datenschutzgrundverordnung”, Art. 4, Rec 24-32.

obliged to observe the legal framework of the processing and to take technical and organisational measures to protect the data.¹³¹

Anonymisation is usually reached by irrevocably removing the identifying characteristics of data to the extent that no re-identification is possible, also not by means of statistical information. For instance, data of several data subjects can be combined to reach aggregated average-values which are then exclusively further used. In this example, the anonymisation process would need to be additionally safeguarded by ensuring a sufficient minimum of data subjects with the same characteristic, or the same combination of several characteristics in order to avoid extreme values.¹³² However, caution should be exercised in the premature assumption that certain data are already anonymous because the identification element is missing. As long as this element can still be found and the data can be re-identified, this qualifies as pseudonymisation at best, but not as anonymisation.

Anonymisation is therefore an activity aiming at achieving a state of anonymity. It preserves the content of a data record, but no longer allows the information to be attributed to a specific or identifiable person. Similar to the aforementioned assessment for the qualification of personal data in Sec 3.2.1.1, the question remains, if the inability to identify a natural person needs to be absolute (meaning nobody on earth can identify the data subject) or relative (the involved stakeholders can no longer identify an individual). As a ground rule, dogmatically, the requirements for valid anonymisation cannot be higher than the requirements to qualify as personal data.

Hence, in essence, the GDPR does not require absolute anonymity. Therefore, factual anonymisation must be sufficient as long as so many features are removed that identification can no longer be achieved with a reasonably expected and not disproportionate effort.¹³³ Taking a closer look at these efforts, the GDPR foresees that in order to determine whether a natural person is identifiable, account should be taken of all means that are likely to be used by the controller or another person, according to general judgement, to identify the natural person directly or indirectly. Furthermore, in order to determine whether means are reasonable and likely to be used to identify the natural person (no disproportionate effort), account should be taken of all objective factors, such as the cost of the identification and the time taken for it, taking into account the technology available at the time of processing.

Further focus should be concentrated on the rapidly enhancing technology and technological developments with its constantly increasing possibilities of assigning apparently anonymous data to the data subjects by technical means (e.g. by comparison with other databases). In fact, there have been raising concerns stating that there is virtually no more room to argue in favour of a disproportionate effort.¹³⁴ This would indeed lead to the conclusion that anonymisation is no longer possible, which is contrary to the legislator mentioning anonymised data in Recital 26 Sentence 5 GDPR. Hence, although techniques to anonymise personal data are subject to technical development, the concept of anonymisation is and remains legally possible.

¹³¹ *Hammer/Knopp*, "Datenschutzinstrumente", DuD 2015, 503; *Karg*, "Anonymität, Pseudonyme und Personenbezug revisited?", DuD 2015, 522.

¹³² *Klar/Kühling*, Kühling/Buchner, "DSGVO", Art. 4 Rec 16.

¹³³ *Plath/Schreiber*, Plath, "BDSG/DSGVO", § 3 BDSG, Rec 56, 59.

¹³⁴ *Ernst*, Paal/Pauly, "DS-GVO", Art. 4, Rec 50.

3.2.8 Phased Approach to handle Personal Data

In conclusion, the previous assessment has shown that privacy and data protection pose significant practical legal issues for Open Science in transport research. Furthermore, details on the interaction between privacy issues and the fundamental principle of research integrity will follow shortly.

Remaining with aspects of privacy and data protection, the evaluation in this deliverable merely focusses on the usability of personal data without pointing out the organisational obligations resulting from legitimate processing of personal data. To at least mention a fraction of such GDPR obligations: apart from fulfilling the basic data protection principles mentioned in Sec 3.2.3, from applying and maintaining technical and organisational safety measures briefly touched in Sec 3.4.1, as well as implementing mandatory contractual structures touched upon in Sec 3.2.2.3, controllers must also deal with

- data subject access requests as well as other rights of the data subjects,¹³⁵
- information obligations to the data subjects,¹³⁶
- organisational documentation of processing activities¹³⁷ including risk-based data protection impact assessments,¹³⁸ and
- data-breach obligations and precautions.¹³⁹

Consequently, personal data cause legal issues for Open Science and should only be processed if the personal data is required for the validity of the research. Hence, it is recommendable to introduce a phased approach for handling of data in the context of Open Science, which also serves to avoid unnecessary efforts as well as the aligned costs for compliance with the GDPR requirements and minimise the risk of all involved actors.

For this phased approach:

- primarily, it must be assessed, if information qualifies as personal data at all (see Sec 3.2.1.1);
- if that is the case, it should be assessed, if the personal data necessarily needs to relate to an identifiable natural person. If that is not the case, then the data should be carefully anonymised (see Sec 3.2.7); and
- If personal data is necessary and/or anonymisation is technically impossible, then a legal basis must be found allowing the processing for the intended purposes (see Sec 3.2.4).

This approach can be summarised as illustrated in the following figure:

¹³⁵ Chapter 3 GDPR.

¹³⁶ See i.e. Art 13, 14 GDPR.

¹³⁷ Art 30 GDPR.

¹³⁸ Art 30 GDPR.

¹³⁹ Art 33, 34 GDPR.

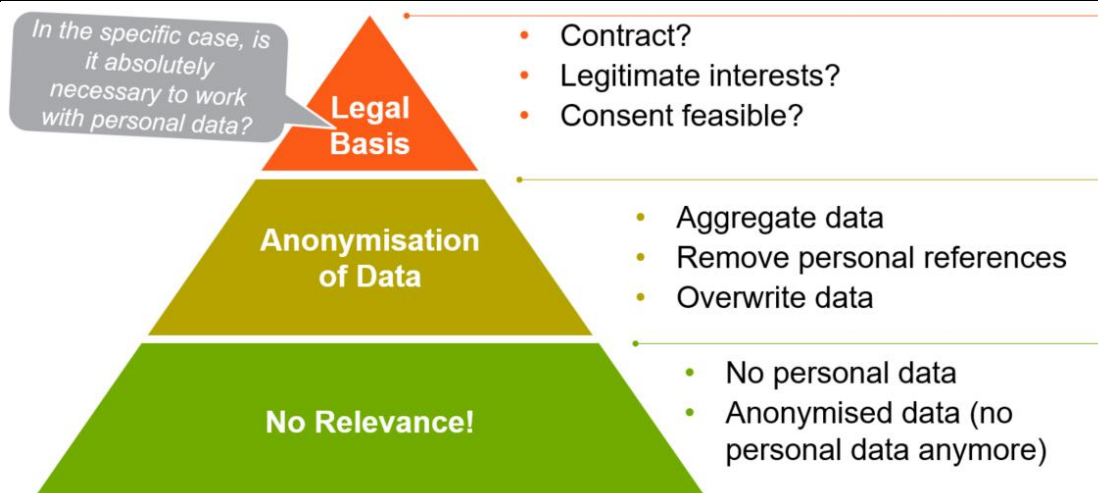


Figure 14 Overview on phased Approach to handle Personal Data

3.3 E-Privacy

The relevant EU legal privacy framework applying to the processing of data is complemented by the Directive on privacy and electronic communications (“**e-Privacy Directive**”).¹⁴⁰ Other than the GDPR, the e-Privacy Directive does not apply directly but rather needs to be transposed by the EU Member States. EU Member States were obliged to transpose the e-Privacy Directive into their national laws by 25 May 2011. Whereas the scope of the GDPR is limited to the processing of personal data,¹⁴¹ the e-Privacy Directive applies to information in general without regard to the nature of such information and thus includes personal and non-personal data.¹⁴²

Most of the provisions of the e-Privacy Directive address providers of publicly available electronic communication services and providers of public communication networks. However, as the overarching aim of the e-Privacy Directive lies in ensuring the protection of fundamental rights and freedoms of subscribers and users with regard to the use of electronic communication networks, the e-Privacy Directive is more far-reaching than one might expect at first sight. Indeed, by means of general provisions, such as Art 5 Para 3 (governing the storage of information and the access to information on terminal equipment) and Art 13 (regulating direct marketing communication), the e-Privacy Directive extends its personal scope to website operators, businesses and entities in general and is consequently relevant in the field of Open Science in transport research.¹⁴³

¹⁴⁰ Directive 2002/58/EC as revised by Directive 2009/136/EC.

¹⁴¹ See Sec 3.2.1.1 for further information on the qualification of data as personal.

¹⁴² For Art 5 Para 3 e-Privacy Directive see, CJEU judgement of 1 October 2019 – C-673/17 (“Planet49”), Rec 70; European Commission study 30-CE-0527128/00-79, “ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation”, P 52 et seq.

¹⁴³ European Data Protection Board, “Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities”, P 11, edpb.europa.eu/sites/edpb/files/files/file1/201905_edpb_opinion_eprivacydir_gdpr_interplay_en_0.pdf, last accessed 14 August 2020; European Data Protection Board, “Guidelines 1/2020 on processing personal data in

3.3.1 Processing of Information

Originally focusing on technologies such as cookies, the material scope of the e-Privacy Directive is in fact considerably broader and includes new economic and technological developments, which the European legislator may not have had in mind when adopting the Directive. However, these developments, including the Internet of Things (“IoT”), increasing machine-to-machine communication, Industry 4.0 and artificial intelligence, have to be taken into account. Hence, in addition to the GDPR governing the processing of personal data, the requirements and prerequisites of the e-Privacy Directive must also be taken into account within the scope of Open Science in transport research.

3.3.1.1 Relationship with the GDPR

According to Art 95 GDPR, in relation to matters for which they are subject to specific obligations with the same objectives set out in the e-Privacy Directive, the GDPR does not impose additional obligations on natural or legal persons in relation to processing connected with the provision of publicly available electronic communications services in public communication networks within the EU. Hence, less dogmatically, Art 95 GDPR delimitates its scope of application with regard to the e-Privacy Directive in the event of a conflict of laws, which may only exist if both legal acts contain competing obligations that pursue the same objective. In this case, Art 95 GDPR stipulates that the provisions of the e-Privacy-Directive take precedence.¹⁴⁴ However, to the extent that the e-Privacy Directive exceeds the scope of the GDPR, both legal acts remain applicable.¹⁴⁵

The GDPR aims at protecting the fundamental rights and freedoms of natural persons and in particular, their right to the protection of personal data as guaranteed in Art 8 Para 1 EU CFR.¹⁴⁶ In contrast, Art 5 Para 3 e-Privacy Directive aims to protect users from interference with their private sphere as guaranteed in Art 7 EU CFR¹⁴⁷ regardless of the nature of the data involved.¹⁴⁸ Thus, Art 5 Para 3 e-Privacy Directive and any EU Member State law transposing this provisions exceeds the scope of the GDPR and by that remain unaffected by the GDPR.¹⁴⁹

3.3.1.2 Storage of and Access to Information

Art 5 Para 3 e-Privacy Directive requires EU Member States to ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed based on the subscriber’s or user’s prior informed consent.

Terminal equipment, as defined in Art 1 lit a Directive 2008/63/EC, means any equipment directly or indirectly connected to the interface of a public telecommunications network to send, process or

the context of connected vehicles and mobility related applications”, Version 1.0, P 5, edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202001_connectedvehicles.pdf, last accessed 14 August 2020.

¹⁴⁴ Klar, Simitis/Hornung/Spiecker gen. Döhmman, „Datenschutzrecht“, Art. 95, Rec 1, 17.

¹⁴⁵ German Federal Court of Justice, decision of 28 May 2020 – I ZR 7/16 (“Cookie-Einwilligung II”), Rec 59.

¹⁴⁶ Art 1 Para 2 and Recital 1 and 2 GDPR.

¹⁴⁷ Formerly Art 8 Para 1 EU CFR.

¹⁴⁸ CJEU judgement of 1 October 2019 – C-673/17 (“Planet49”), Rec 70; see also Recital 24, 25 e-Privacy Directive.

¹⁴⁹ See German Federal Court of Justice, decision of 28 May 2020 – I ZR 7/16 (Cookie-Einwilligung II”), Rec 58 et seq.

receive information. Hence, any device connected to public electronic communications network qualifies as terminal equipment. In contrast, facilities that are not connected to a public communications network are not covered by this provision.

In its recent opinion, the European Data Protection Board specifically pointed out that the aforementioned definition includes connected vehicles and any devices connected to them.¹⁵⁰ This emphasises the relevance for stakeholders with regard to Open Science in transport research.

Exemptions from the requirement of informed consent only apply if

- data is stored or accessed for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or
- the data storage or access is strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.

3.3.1.3 Informed Consent

Art 5 Para 3 e-Privacy Directive does not indicate the way in which consent must be given. However, Art 2 lit f e-Privacy Directive, which defines the term “consent” for the purpose of the e-Privacy Directive refers to the former Directive on the protection of individuals with regard to the processing of personal data (“**Data Protection Directive**”¹⁵¹).¹⁵² Hence, consent within the meaning of Art 3 Para 3 e-Directive has the same meaning as the data subject’s consent defined and further specified in the Data Protection Directive.¹⁵³ To complete the chain of statutes, as the GDPR has repealed the Data Protection Directive, the definition provided in Art 4 No 11 GDPR is now the decisive provision to determine the term “consent”, also within the scope of the e-Privacy Directive.¹⁵⁴ Consequently, the notion of consent in the e-Privacy directive remains the notion of consent in the GDPR and must meet all the requirements of consent as provided by Art 4 No 11 and Art 7 GDPR.¹⁵⁵

In context of Open Science in transport research, stakeholders will in most cases not be able to rely on the statutory exemptions provided by Art 5 Para 3 e-Privacy Directive and thus will be required to obtain the end user’s consent. To recall, consent is required regardless of whether the data is considered personal data. Regarding consent, they then have to observe the same aspects as with consent pursuant to the GDPR and may consequently be confronted with the same legal obstacles.

In light of complex interaction between the e-Privacy Directive and the GDPR, where personal data is concerned, any processing following the storage of data or access to data in the user’s terminal

¹⁵⁰ European Data Protection Board, “Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications”, Version 1.0, 28 January 2020, P. 5, edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202001_connectedvehicles.pdf, last accessed 14 August 2020.

¹⁵¹ Directive 95/46/EC.

¹⁵² See also Recital 17 Directive 2002/58/EC, Recital 66 Directive 2009/136/EC.

¹⁵³ CJEU judgement of 1 October 2019 – C-673/17 (“Planet49”), Rec 50.

¹⁵⁴ Ibid, Rec 70; German Federal Court of Justice, decision of 28 May 2020 – I ZR 7/16 (“Cookie-Einwilligung II”), Rec 63.

¹⁵⁵ See Sec 3.2.4.1 **Error! Reference source not found.** for further details on the requirements for valid consent.

equipment additionally requires a legal basis pursuant to Art 6 Para 1 or Art 9 Para 2 GDPR. This includes processing of personal data obtained by accessing information in the terminal equipment.¹⁵⁶

3.3.2 Dissemination

The legal assessment of the BE OPEN dissemination strategy, which is an essential aspect of BE OPEN work package WP 6 showed that e-Privacy aspects based on EU Member State legislation transposing the e-Privacy Directive are of essential interest to Open Science in transport research stakeholders. Apart from aspects of dropping cookies on a website, the e-Privacy aspects are of particular interest in regards to all electronic communication that qualify as marketing communication.

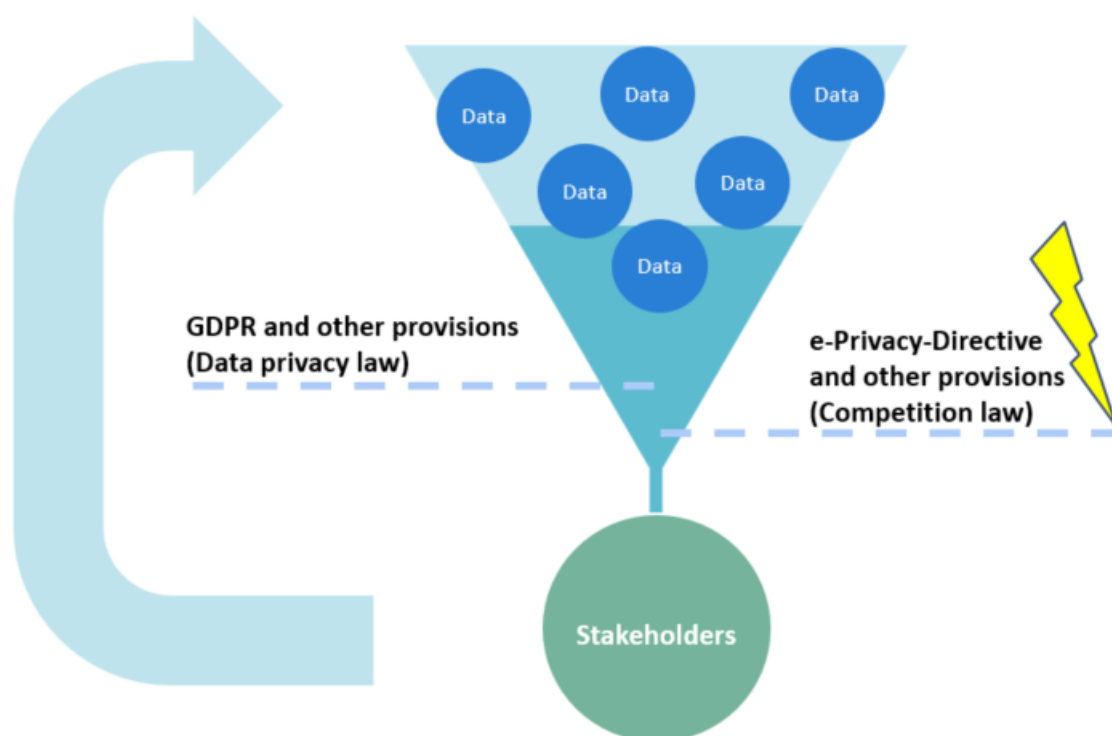


Figure 15 Interlink between GDPR and e-Privacy Directive

Here, based on Art 13 e-Privacy Directive, the EU Member States have passed laws, which have in common the broad interpretation of a marketing purpose, which can also cover electronic communication activities in the field of Open Science in transport research. Marketing purposes are defined by

¹⁵⁶ European Data Protection Board, “Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities”, P 14, edpb.europa.eu/sites/edpb/files/files/file1/201905_edpb_opinion_eprivacydir_gdpr_interplay_en_0.pdf, last accessed 14 August 2020; European Data Protection Board, “Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications”, Version 1.0, P 5, edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202001_connectedvehicles.pdf, last accessed 14 August 2020.

D4.1: Open Science in transport research: legal issues and fundamental principles

the Directive on misleading and comparative advertising¹⁵⁷ as “*the making of a representation in any form in connection with a trade, business, craft or profession in order to promote the supply of goods or services, including immovable property, rights and obligations.*”

Essentially, this broad marketing interpretation does not require direct sales promotion, making any form of indirect sales promotion sufficient. Hence, it also applies to image advertising and sponsoring, which in an Open Science context can also be applicable for non-profit researchers and research institutes when electronic communication e.g. through a e-mail newsletter helps them gain funding for their projects.¹⁵⁸

As a ground rule, all electronic communications activities qualifying as marketing require explicit consent by the targeted individual. However, for the sake of completeness, most EU Member States have introduced nearly similar exceptions for e-mail-marketing towards existing customers within narrow legal limits and exemptions on presumed consent for telephone-marketing in a business context. These exemptions are however not of high relevance to Open Science in transport research.

Hence, where dissemination leads to direct marketing activities involving electronic communication, stakeholders must be aware that these activities generally require valid consent. Furthermore, stakeholders must keep in mind that e-Privacy obligations apply in addition to any GDPR requirements.

3.4 Security Aspects

Security aspects can be both, of legal and non-legal nature and may consist of ethical aspects. Standards and certification schemes act as important intermediary between these legal and non-legal security aspects and can facilitate compliance with requirements arising from both worlds. As such, the ISO/IEC 27000 series issued by the International Standards Organisation ("ISO") and the International Electrotechnical Commission ("IEC") are of particular practical importance and help stakeholders demonstrate to the regulators and to their customers that appropriate security measures and organisational processes have been implemented.

Mandatory security aspects can arise from various different legal angles. All security certifications have in common, that they cannot replace mandatory regular assessment of whether or not legal requirements subject to regular adjustment are sufficiently up-to-date.

As outlined in the following figure and further assed upon hereinafter, legal security aspects require a risk assessment and have in common, that they require an adequate balance of compliance with legal requirements, application of sufficient technical and/or organisational measures as well as resulting costs of implementation and maintenance of efficient security aspects.

¹⁵⁷ Directive 2006/114/EC

¹⁵⁸ *Fritzsche*, Fritzsche/Müncker/Stollwerk, “BeckOK UWG“, § 7 UWG, Rec 45.

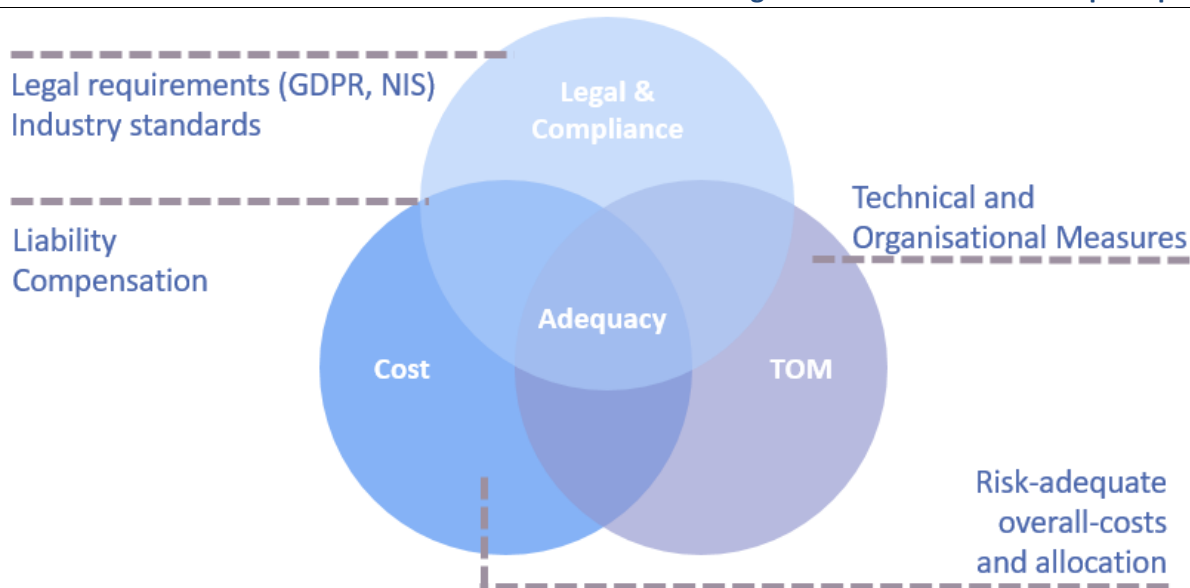


Figure 16 Overview on adequate Implementation of Security Aspects

3.4.1 Privacy related Security Aspects

3.4.1.1 Context and Scope of Application

Since the BE OPEN surveys showed that privacy aspects pose the biggest barrier to Open Science in the eye of most stakeholders¹⁵⁹, the existing legal security obligations resulting from processing of personal data under the GDPR are of high importance when determining legal issues.

3.4.1.2 Risk-based Approach for Security Aspects

The GDPR follows a risk-based approach of adopting mandatory technical and organisational measures without explicitly mentioning a full set of requirements. On the technical side, the GDPR requires implementing privacy-by-design and privacy-by-default measures. On the organisational side, the GDPR mainly requires the implementation of effective organisational procedures for providing transparent and accurate information, securing the mandatory contractual privacy structures, safeguarding proper handling of (potential) data breach incidents, data protection impact assessments, maintaining proper records of processing and fulfilling data subject requests.

The technical and organisational measures required by Art 24 Para 1 GDPR are specified in Art 32 Para 1 GDPR in broad technical terms. The mandatory risk-based approach¹⁶⁰ of determining appropriate technical and organisational measures shall be based on the state of the art, the costs of implementation, the nature, scope, context, ad purposes of the processing, and the risk of varying likelihood and severity for the rights and freedoms of natural persons.

¹⁵⁹ BE OPEN deliverable D 2.2, "Open/FAIR data, software and infrastructure in European transport research", P 38.

¹⁶⁰ Paulus, Wolff/Brink, "BeckOK DatenschutzR DS-GVO", Art. 32 Rec 7.

D4.1: Open Science in transport research: legal issues and fundamental principles

Such a risk-based approach must also take into account the basic principles relating to processing of personal data (see Sec 3.2.3), and may even conflict with the aforementioned basic principles of data protection. Exemplary, this can be the case where the principle of data minimisation¹⁶¹ requires storing data only in one single space and the security of processing requires providing for the ability to restore data, which is usually achieved by means of a secondary backup. Such circumstances call for an appropriate balancing of risks for the involved individuals. Providing guidelines for the proper determination of adequate security measures, the GDPR holds broad suggestions in Art 32 Para 1 GDPR. The mentioned measures are:

- the pseudonymisation and encryption of personal data;
- the ability to ensure the on-going 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; and
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

The concrete measures to be taken will depend very much on the individual case. Any measures taken may in turns have the effect of reducing fines. In this case, it is advisable to follow on from the evaluations of the ISO 27001¹⁶² audit and to supplement specific measures indicated in terms of data protection law if this proves necessary.¹⁶³ Possible technical measures are:

- Implementation of data protection through technology design in the system architecture.
- Technical implementation of the principles of purpose limitation and data minimisation.
- Introduction of a data retention and erasure schedule.
- Establishment of a central register of stored personal data, which also serves to answer the inquiries of data subjects.
- Definition of a data protection compliant IT procurement process.
- Creation or adaptation of a policy for IT security in accordance with the requirements of data protection law.

Furthermore, technical measures should be safeguarded by accompanied organisational measures in order to avoid circumvention of technical security measures by human interaction.¹⁶⁴

¹⁶¹ Art 5 Para 1 lit c GDPR.

¹⁶² For information about ISO 27001, see: www.iso.org/isoiec-27001-information-security.html, last accessed 14 August 2020.

¹⁶³ *Reto/Mantz, Sydow, "Europäische Datenschutzgrundverordnung", Art. 32, Rec 10.*

¹⁶⁴ *Martini, Paal/Pauly, "DS-GVO", Art. 24 Rec 22.*

3.4.2 Security Aspects under the Network Information Security Directive

3.4.2.1 Context and Requirements for Security

The Directive on security of network and information systems (“**NIS Directive**”)¹⁶⁵ entered into force in August 2016. EU Member States were obliged to transpose the Directive into their national laws by 9 May 2018 and had to identify the subjects falling into the scope of these national laws by 9 November 2018.¹⁶⁶ Currently, the functioning of the Directive is under periodical review, which will conclude in an impact assessment by the end of 2020. As part of this process, a consultation opened on 7 July 2020, with as deadline 2 October 2020.

This EU legislation aims to develop a common approach across Europe to address the potential for socio-economic damage caused by attacks on network and information systems of Operators of Essential Services (“**OES**”) and Digital Service Providers (“**DSP**”). As such, the NIS Directive provides legal measures to enhance the overall level of cybersecurity in the EU by ensuring:¹⁶⁷

- EU Member States are sufficiently prepared and appropriately equipped, e.g. via a Computer Security Incident Response Team (“**CSIRT**”)¹⁶⁸ and a competent national NIS authority,¹⁶⁹
- institutional cooperation among all the EU Member States, in order to support and facilitate strategic cooperation and the exchange of information among EU Member States. This includes establishing a CSIRT Network, in order to promote swift and effective operational co-operation on specific cybersecurity incidents and sharing information about risks;
- a culture of security across sectors that are identified as vital for the economy and society in the EU, such as transport infrastructure. Stakeholders in sectors identified as operators of essential services will have to take appropriate security measures and undertake to notify serious incidents to the relevant national authority. Also key DSP (search engines, cloud computing services and online marketplaces) will have to comply with the security and notification requirements under the directive and the respective transposed EU Member State laws.

Similar to the aforementioned privacy security aspects, the NIS Directive also follows a risk-based approach and requires EU Member States to implement legislation for security measures taking into account the state of the art, ensuring a level of security of network and information systems adequate to the risk. This includes¹⁷⁰:

- appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in their operations.

¹⁶⁵ Directive (EU) 2016/1148.

¹⁶⁶ Information on the EU Member State transposition status is available at ec.europa.eu/digital-single-market/en/state-play-transposition-nis-directive; last accessed 14 August 2020.

¹⁶⁷ See: ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive; last accessed 14 August 2020.

¹⁶⁸ Art 9 NIS Directive.

¹⁶⁹ Art 8 Para 3 NIS Directive.

¹⁷⁰ Art 14, 15 NIS Directive.

D4.1: Open Science in transport research: legal issues and fundamental principles

- that operators of essential services take appropriate measures to prevent and minimise the impact of incidents affecting the security of the network and information systems used for the provision of such essential services, also ensuring the continuity of those services; and
- that operators of essential services notify, without undue delay, the competent authority or the CSIRT of incidents having a significant impact on the continuity of essential services.

Furthermore, the EU Commission makes information on the Member States' national strategy on the security of network and information systems available.¹⁷¹

3.4.2.2 NIS Directive Scope of Application

The NIS Directive applies to both OES and DSP. For the transport sector, the OES determined by each Member State are of particular importance because Stakeholders from this sector are within the envisaged scope of the NIS Directive under Annex II of the Directive. Furthermore, private and public entities can fall within the scope of an OES¹⁷² if the stakeholder is:

- an entity providing a service which is essential for the maintenance of critical societal and/or economic activities,
- the provision of that service depends on network and information systems, and
- an incident would have significant disruptive effects on the provision of that service.¹⁷³

In regards to such disruptive effects, the NIS Directive holds further specifications, mandating the EU Member States to consider the following factors when determining the significance of a disruptive effect:¹⁷⁴

- the number of users relying on the service provided by the entity concerned;
- the dependency of other sectors referred to in Annex II on the service provided by that entity;
- the impact that incidents could have, in terms of degree and duration, on economic and societal activities or public safety;
- the market share of that entity;
- the geographic spread with regard to the area that could be affected by an incident;
- the importance of the entity for maintaining a sufficient level of the service, taking into account the availability of alternative means for the provision of that service.

The following transport sector modes are explicitly considered in the NIS Directive:¹⁷⁵

¹⁷¹ See ec.europa.eu/digital-single-market/en/state-play-transposition-nis-directive, last accessed 14 August 2020.


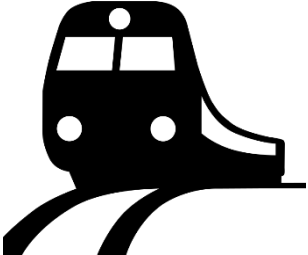
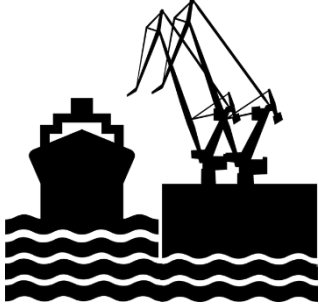
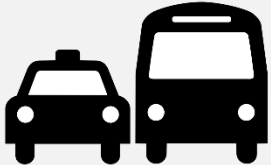
¹⁷² Art 4 Para 4 NIS Directive.

¹⁷³ Art 5 Para 1 NIS Directive.

¹⁷⁴ Art 6 Para 1 NIS Directive.

**D4.1: Open Science in transport research:
legal issues and fundamental principles**

Table 4 Transport Sector Modes covered by NIS Directive

TRANSPORT SECTOR MODE	TYPE OF ENTITY	EU SOURCES FOR ENTITIES
 AIR	Air carriers	Point (4) of Article 3 of Regulation (EC) No 300/2008
	Airports and airport managing bodies and entities operating ancillary installations contained within airports	Point (1) and (2) of Article 2 of Directive 2009/12/EC; including the core airports listed in Section 2 of Annex II to Regulation (EU) No 1315/2013
	Traffic management control operators providing air traffic control service	Point (1) of Article 2 of Regulation (EC) No 549/2004
 RAIL	Infrastructure managers	Point (2) of Article 3 of Directive 2012/34/EU
	Railway undertakings and operators of related service facilities	Points (1) and (12) of Article 3 of Directive 2012/34/EU
 WATER	Inland, sea and coastal passenger and freight water transport companies	Annex I to Regulation (EC) No 725/2004, not including the individual vessels operated by those companies
	Managing bodies of ports including their port facilities and entities operating works and equipment contained within ports	Point (1) of Article 3 of Directive 2005/65/EC; point (11) of Article 2 of Regulation (EC) No 725/2004
	Operators of vessel traffic services	Point (o) of Article 3 of Directive 2002/59/EC
 ROAD	Road authorities responsible for traffic management control	Point (12) of Article 2 of Commission Delegated Regulation (EU) 2015/962
	Operators of Intelligent Transport Systems	Point (1) of Article 4 of Directive 2010/40/EU

¹⁷⁵ Annex II, NIS Directive.

D4.1: Open Science in transport research: legal issues and fundamental principles

To conclude, this evaluation shows, that public and private operators active in the transport sector may very well qualify as OES and as such fall within the scope of the respective EU Member State laws implementing the NIS Directive.

The second subject of application are DSP. In contrast to the OES, there is no assessment of such services by the EU Member States. Defining the scope of a digital service, the NIS Directive refers to the definition in Directive (EU) 2015/1535 covering any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services.¹⁷⁶ Hence, online businesses must self-assess whether or not they fall within the scope NIS Directive as online marketplace, online search engine, or cloud computing service.

In conclusion, the definition of a DSP shows that stakeholders in the Open Science transport sector are unlikely to fall directly within the scope of the NIS Directive as DSP. Notwithstanding, EU Member State laws implementing the NIS Directive may indirectly apply to suppliers of OES and/or DSP as a result of flow-down obligations.

3.4.2.3 Conclusion

In conclusion, both examined legal security aspects based on EU Member State laws or EU regulations generally require:

- a risk based approach of regularly assessing associated risks,
- procedures of regularly checking if technical and organisational risk-mitigating measures not only fulfil the broad description of a legal requirement but rather remain state-of-the-art,
- establish and maintain training and reporting procedures for identifying risks and assessing on mitigating actions,
- establish and maintain procedures to sufficiently handle breach-related obligations i.e. based on the GDPR and EU Member State laws transposing the NIS Directive, and
- consulting experts and regularly assess the available of current industry-standards for security measures.

4 Non-legal Aspects

Even though legal issues and as such especially privacy aspects have been determined as the main barriers towards the adoption of Open and FAIR data principles in Open Science in transport research by various BE OPEN deliverables, the assessment has shown that non-legal aspects are also capable of posing important obstacles.¹⁷⁷

Such non-legal aspects can arise from many different angles. Particularly, they can be of theoretical and practical nature and can be directly or indirectly visible as barrier to Open Science. Highly practi-

¹⁷⁶ Art 4 Para 5 NIS Directive in connection with Art 1 Para 1 lit b Directive (EU) 2015/1535.

¹⁷⁷ BE OPEN deliverable D 2.4, “Governance and operational models”, P 33 et seq.

D4.1: Open Science in transport research: legal issues and fundamental principles

cal and directly visible issues have been determined in BE OPEN surveys with stakeholders from the transport sector.

These surveys outlined that a key requirement for promoting the re-use of data as well as sharing data and infrastructure is simply the good quality of the published data.¹⁷⁸ Sufficient data quality was also determined as important to enable data re-use in light of engaging stakeholders from different fields, hence broadening the scope of research-data usage.¹⁷⁹ The non-legal aspect of anticipated mistrust in the quality of data can furthermore minimise the essential benefits of Open Science in transport research, which include effective and cost-saving research, unnecessary duplication of research and even the reduction of scientific fraud. In fact, BE OPEN surveys have shown that mistrust in the quality of Open Data can lead researcher to turn away from the idea of Open Science in its entirety, or to minimise the benefit of Open Science by routinely double-checking the validity of each and every content. These concerns were explicitly voiced in BE OPEN surveys as follows¹⁸⁰:

- *“Publications are of dubious quality.”*
- *“Open publications should often get double-checked to validate their content.”*
- *“Open data are not necessarily validated, so they are simply not trusted to be used.”*
- *“... (in order) to increase the use of open data, one would need to guarantee their quality” and “accuracy/quality, novelties, availability and cost of open data are major elements for increasing their use.”*

To state an obvious fact, in order to reduce the essential non-legal issue of mistrust in the quality of data, this quality of Open Data in Open Science must be enhanced on a broad scale. In pursuit of this goal, there are various approaches. For instance, there are arguments, stating that Open Science in transport research requires precisely defined data, adjusted incentives and efficient training of researchers in order to use Open Science databases. Furthermore, data collection standards, metadata, infrastructure and functional requirements should be subject to definition in order to ensure an appropriate level of service.¹⁸¹

Notwithstanding, these approaches are supplementary to the basic principle that the quality of data can be enhanced and safeguarded by the fundamental principles of research integrity¹⁸² which are essential to Open Science in transport research. Hence, as the assessment in Sec 4.2 will show, complying with fundamental principles of research integrity is a core aspect to enhance the quality of data, which was determined as the key non-legal issue for Open Science. However, since the funda-

¹⁷⁸ BE OPEN deliverable D 2.1, “Open Access Publications and the Performance of the European Transport Research”, P 30.

¹⁷⁹ BE OPEN deliverable D 1.2, “Open Science Framework Terminology and Instruments”, P 37.

¹⁸⁰ BE OPEN deliverable D 2.4, Governance and operational models, P 33.

¹⁸¹ G. Yannis, M. Böhm, J. R. Franklin, S. Jones, T. Kovacicova, K. Nowicka, K. Folla, “Exploring the Establishment of a European Transport Research Cloud”, 9th International Congress on Transportation Research, 24th-25th October, Athens, Greece; BE OPEN deliverable D 2.4, Governance and operational models, P 29.

¹⁸² See The European Code of Conduct for Research Integrity, [ec.europa.eu/research/participants-data/ref/h2020/other/hi/h2020-ethics_code-of-conduct_en.pdf](https://ec.europa.eu/research/participants/data/ref/h2020/other/hi/h2020-ethics_code-of-conduct_en.pdf), last accesses 14 August 2020.

mental principles of research integrity are itself a description of an ethical attitude with particular focus on scientists, first the focus will be on broader ethical concerns in- and outside the research community. This assessment is primarily determined to evaluate the likelihood of broad ethical concerns qualifying as significant barriers for Open Science in transport research.

4.1 Ethical Concerns

In pursuit for a broader definition of ethics, sociologically, ethics relates to an evaluation of which actions are generally perceived as right or wrong within a comparable environment. In particular, the respective community one forms part of can set this environment. Hence, ethics can be described as evaluative aspect attached to an individual within society as well as to the organisations (e.g. public authorities and companies) active within this society, pointing towards their moral conduct.¹⁸³

4.1.1 Interaction between Ethics and the Law

Against the background of this definition, it becomes evident, that most societies have adopted legal systems that are capable of flexibly adopting laws that efficiently ban what is considered unethical and permit what is considered ethical (or at least not unethical). In practice, this entails that each individual or organisation going against what is ethically acceptable may be legally punished.

This close connection between ethical aspects and aligned legal jurisdiction provides an explanation for the fact that legal aspects such as IPR and data protection have been mentioned as essential ethical aspects for Open Science in transport research during the BE OPEN document review.¹⁸⁴ Essentially, in a 2018 survey conducted among 87 researchers of academic institutions, representatives of public authorities and stakeholders of the commercial sector in 29 European countries, asked to explain ethical issues, most of the respondents mentioned data protection issues. In particular, participants declared that while data should be available for research purposes, some data (e.g. survey data) might be sensitive due to data privacy issues and thus, restrictions should exist in some cases, which could be ensured by permitting access only to aggregated data.¹⁸⁵

This assessment is largely in line with the proposed phased approach to handling personal data in Sec 3.2.8, although the aggregation of data is only one amongst various ways to anonymise data.¹⁸⁶

4.1.2 Non-legal Aspects of ethical Concerns

Apart from the aforementioned ethical concerns that are explicitly addressed as legal issues, there are several other ethical concerns associated with Open Science or publishing research data in general. Many however mirror or intensify existing concerns about publishing research data and are not explicitly connected to the transport sector. For instance, publishing data without restrictions may in

¹⁸³ See *Julien Debussche/Jasmien César/Min-Sung Hong et.al., "Report on Ethical and Social Issues for Horizon 2020", LEMO deliverable, P 6.*

¹⁸⁴ This document review can be found in BE OPEN deliverable D 2.1, "Open access publications and the performance of the European transport research".

¹⁸⁵ *Ibid*, P. 22.

¹⁸⁶ See Sec 3.2.7 for further information on anonymisation.

D4.1: Open Science in transport research: legal issues and fundamental principles

some cases conflict with established principles of ethical research, including respect for the autonomy of individuals, justice and beneficence.¹⁸⁷

Historically, codes of ethics have a long ranging history in the research society, predominantly derived from the field of medical sciences, where ethical standards for research have evolved governing primarily medical experiments on humans. Beginning with the Nuremberg Code¹⁸⁸ which was a reaction to medical experiments in Nazi concentration camps, the Declaration of Helsinki on Ethical Principles for Medical Research Involving Human Subjects¹⁸⁹ was subsequently adopted in 1964 and has been amended ever since. Today, codes of ethics have evolved in different fields, both in the public and private sector, urging researchers to sufficiently inform participants about the nature of their research activity, treat data confidentially and ensure equal distribution of benefits and burdens of research.¹⁹⁰ It is agreed, that any failure to meet such ethical standards may not only cause harm to the participants in the research activity but may rather even be detrimental to the scientific enterprise or society in a whole.¹⁹¹ As such, Finn, Wadhwa, Taylor et al, have determined five additional ethical aspects which have not been raised in the surveys carried out in the BE OPEN project. Essentially, these exemplary aspects are not connected to transport research but can however be applied to issues from the transport sector and thus serve as basis for transport-sector examples.

These aspects are:¹⁹²

- **Unintended secondary uses and misappropriation.** Although secondary use combines some of the benefits of Open Science such as validating information and keeping it up-to-date, unintended use bears ethical risks as to misinterpretation of data. Practical aspects of misinterpretation may exemplary arise when data is further processed out of context and used for purposes that the initial researcher or involved participants do not agree with.
 - In regards to research participants, unintended secondary use is particularly problematic when highly sensible personal data is involved which can ultimately lead to stigmatisation, discrimination or other physical damage to an individual's health and wellbeing.
 - Looking at researchers, unintended secondary use can significantly harm the reputation of an individual researcher or even the entire associated institution.

¹⁸⁷ Finn/Wadhwa,/Taylor et al, "Legal and ethical issues in open access and data dissemination and preservation, Policy RECommendations for Open access to research Data in Europe", deliverable D 3.1, P 33.

¹⁸⁸ Shuster, "Fifty Years Later: The Significance of the Nuremberg Code", www.nejm.org/doi/full/10.1056/NEJM199711133372006, last accessed 14 August 2020.

¹⁸⁹ See www.wma.net/policies-post/wma-declaration-of-helsinki-ethical-principles-for-medical-research-involving-human-subjects, last assessed 14 August 2020.

¹⁹⁰ E.g. for private sector, see Microsoft's AI and Ethics in Engineering and Research (AETHER) Committee, news.microsoft.com/2018/03/29/satya-nadella-email-to-employees-embracing-our-future-intelligent-cloud-and-intelligent-edge/, last accessed 14 August 2020.

¹⁹¹ Finn/Wadhwa,/Taylor et al, "Legal and ethical issues in open access and data dissemination and preservation, Policy RECommendations for Open access to research Data in Europe", deliverable D 3.1, P 33

¹⁹² Ibid, P.34 et seqq.

D4.1: Open Science in transport research: legal issues and fundamental principles

- **Dual use.** In light of ethics, the concept of dual use poses detrimental risks for the research. Other than the aforementioned ethical risks originating from unintended secondary use and misappropriation, the potential collateral detriment is inherently connected to the research data. In transport research, e.g. information on the amount of passengers of public transportation during peak-times can be beneficial for transport research and may lead to knowledge, products or technologies, which in turns benefit society. However, such information can also be used with ill intent e.g. by terrorist planning attacks on soft targets such as public transportation.
- **Unequal distribution of research results.** Open access to data does not necessarily guarantee that all stakeholders benefit equally. In fact, data may only be formally open while certain groups of researchers lack the required scientific, technical or cultural resources to make use of the data. This is of particular significance for researchers in less developed countries who may not have the technical capacities to access transport research-data although it is theoretically open. Unequal distribution may also be the result of different capacities for putting the data to further use. Exemplary, knowing that only certain regions in the world have the capacities to efficiently provide research on automated driving, could lead researchers from other regions to refrain from making necessary raw-data for automated driving research available as long as they lack the capacities of performing research on automated driving themselves.
- **Commercialisation.** The ability to obtain monetary value from research data as public good can lead to various ethical concerns. On the one hand, public institutions and of such especially universities have developed a commercial mind-set because they gain monetary value from their research. Consequently, universities can be steered in certain directions by interests of private companies because income from the private sector has become increasingly important for universities. Furthermore, universities have also become increasingly active in commercial endeavours such as participating in commercial start-ups. On the other hand, Open Science research data of universities can also be used by private companies who then, without letting the universities participate in the monetary benefits, use this data to develop commercial patents and other valuable goods and services.
- **Restriction of scientific freedom.** There are various ethical concerns about the restriction of scientific freedom. For once, the scientific freedom can be restricted by the aforementioned commercialisation, which leads science in a certain monetary valuable direction. Furthermore, researchers are increasingly dependent on a small set of state-of-the-art IT-tools enabling them to exploit the full potential of Open Science. This can in turns lead to a lock-in of the researchers and negatively influence their scientific freedom of choosing their means and goals of scientific research.

On the plus side it can be concluded that the research community has developed a range of strategies to mitigate some of the ethical concerns, for instance by technical means such as actively monitoring published data by means of de-identifying data through statistical techniques or regulating and monitoring access to research data.

Furthermore, as previously touched upon, broader ethical concerns are mitigated by means of applying the fundamental principles of research integrity in light of the basic ethical principles being well articulated amongst the stakeholders.¹⁹³

4.2 Fundamental Principles of Research Integrity

The fundamental principles of research integrity have a long-standing history within all fields of science. Research integrity is defined as adherence to ethical principles and professional standards for responsible research practices, which mainly consist of honest and verifiable methods in proposing, conducting and evaluating research. For the individual researcher, this integrity is an aspect of moral nature and experience, while for institutions it is about creating an environment that promotes responsible behaviour by setting standards of excellence and trustworthiness.¹⁹⁴

While most universities around the world establish and publish individual guidelines on research integrity¹⁹⁵, within the scope of Open Science, multilateral fundamental principles of research integrity are of great importance. As such, the EU Commission has been engaging in activities to determine unified principles of research integrity, also within the Horizon 2020 programme.¹⁹⁶

As essential groundwork in this field and in cooperation with the EU Commission, a “European Code of Conduct for Research Integrity” has been developed by the European Federation of Academies of Sciences and Humanities which consists of 59 academies from more than 40 countries (“All European Academies - ALLEA”).¹⁹⁷

The code of conduct was essentially published in 2017 and is aimed at applying to research in all scientific and scholarly fields from both publicly funded research and the private research-sector. The framework for self-regulation in the code of conduct consists of:

- definitions for the essential principles of research integrity,
- accompanying good research practices in order to define criteria for proper research behaviour enhancing the quality and reliability of research, and
- guidance on how to handle violations of research integrity enabling an adequate response to threats to, or violations of research integrity

¹⁹³ National Research Council, “Putting People on the Map: Protecting Confidentiality with Linked Social-Spatial Data”, doi.org/10.17226/11865, P 33 et seq, last accessed 14 August 2020.

¹⁹⁴ Francisco/Hahn/Schwarz, “Editorial Wissenschaftliche Integrität”, onlinelibrary.wiley.com/doi/10.1002/ange.201700613, last accessed 14 August 2020.

¹⁹⁵ See e.g. Guidance on Research Integrity by Harvard University, vpr.harvard.edu/pages/research-integrity, last accessed 14 August 2020.

¹⁹⁶ See e.g. Research Integrity in Horizon2020, ec.europa.eu/programmes/horizon2020/en/news/commission-moves-strengthen-research-integrity, last accessed 14 August 2020.

¹⁹⁷ See The European Code of Conduct for Research Integrity, ec.europa.eu/research/participants/data-ref/h2020/other/hi/h2020-ethics_code-of-conduct_en.pdf, last accesses 14 August 2020.

D4.1: Open Science in transport research: legal issues and fundamental principles

ALLEA explicitly recognises that the code of conduct needs to be a living document which serves as baseline whilst being open to regular updates as well as local and national differences in its implementation.¹⁹⁸

According to the code of conduct, the fundamental principles of research integrity aimed at guiding researchers in their work as well as in their engagement with the practical, ethical and intellectual research-challenges are as follows:¹⁹⁹

- **Reliability** in ensuring the quality of research, reflected in the design, the methodology, the analysis and the use of resources.
- **Honesty** in developing, undertaking, reviewing, reporting and communicating research in a transparent, fair, full and unbiased way.
- **Respect** for colleagues, research participants, society, ecosystems, cultural heritage and the environment.
- **Accountability** for the research from idea to publication, for its management and organisation, for training, supervision and mentoring, and for its wider impacts.

Due to their ethical characteristics and connection to both non-legal and legal aspects of Open Science in transport research, the interaction between the fundamental principles of research integrity and the designated legal issues can serve as gateway for the conclusion of this BE OPEN deliverable dealing with Open Science in transport research and focussing on the legal issues and fundamental principles.

5 Conclusions

As presented above, the non-legal barriers to Open Science in transport research²⁰⁰ obviously interact with the fundamental principles of research integrity. Here, especially the growing influence of research commercialisation can conflict with the principle of research objectivity as well as research impartiality, which are essential elements of the determined principles.

In addition, as already touched upon, the fundamental principles of research integrity are capable of interfering with the determined legal issues and can thus lead to indirect barriers for Open Science in transport research. This might be surprising, since both the fundamental principles and main legal aspects have overlapping objectives, such as transparency.

However, an easy privacy-example proves differently: If, for instance a researcher publishes the names and contact details of all participants of a controversial survey, then this can very well serve to promoting the accountability of the research. Then again, openly publishing names and contact details of participants would not only raise ethical concerns but would most likely be an unjustifiable

¹⁹⁸ Ibid, P 3.

¹⁹⁹ Ibid, P 4.

²⁰⁰ In addition to the current section, please also see the determined non-legal aspects in in Sec 2.

D4.1: Open Science in transport research: legal issues and fundamental principles

breach of privacy obligations. Hence, it becomes evident that fundamental principles of research integrity can indeed pose potential barriers to Open Science in the research community.

This interaction between fundamental principles of research integrity and legal aspects can especially become relevant in regards to privacy laws, but also in regards to IPR.

For instance,

- as a result of commercialisation, privately funded transport research can be kept behind closed doors due to IPR aspects which in turns violates the principle of research objectivity requiring researchers to produce data capable of proof and secondary review. Furthermore, privately funded research may foundationally raise concerns in regards to impartiality and independence from the funding party.
- Furthermore, shifting the aforementioned privacy-example to an abstract perspective, while privacy laws acknowledge the concept of anonymity, fundamental principles of research integrity rather focus on promoting accountability, which in turns is diametrically opposed to the concept of anonymity.
- In addition, security obligations regulating how to store and process data may lead to restrictions of the scientific freedoms of choosing the essential scientific means and procedures freely.

Given the importance of both fundamental aspects of research integrity and the determined legal issues, this conflict must be solved by an orderly reconciliation of conflicting interests.

In fact, since legislation is an ongoing procedure, which is highly influenced by ethical aspects, there are indeed many ways of sufficiently balancing the involved interests. For instance within the scope of the GDPR, which has been determined as the essential legal aspect for Open Science in transport research, as the assessment in Sec 3.2.5 has shown, the GDPR explicitly acknowledges the needs of the science-sector.

Even if there is no provision elevating the fundamental principles of research integrity to the rank of law, these principles are very well valued through the balancing of interests as described in Sec 3.2.4.4.

This leads to the conclusion that while personal data should generally be avoided pursuant to the recommended phased approach in Sec 3.2.8, this recommendation mainly applies to personal data of research subjects. Notwithstanding, on the other hand, fundamental principles of research integrity may indeed require that researchers and/or publishers are in fact individualised in order to promote accountability. To the extent that this is not anyways legally required and thus justified in light of IPR or other legal obligations, due to the high importance of fundamental principles of research integrity, the balancing of interests ranking as essential legal basis for Open Science under the GDPR, is likely to shift toward identifying the researcher or publisher.

In conclusion, various legal and non-legal issues interact with fundamental principles of research integrity. In order to resolve this tension, clear legislation and a legal framework supporting intellec-



**D4.1: Open Science in transport research:
legal issues and fundamental principles**

tual property rights, data security, data protection and privacy is imperative. To pave the way towards this objective, the Code of Conduct on Open Science in Transport will be developed by the BE OPEN project in deliverable D 4.4.
