Deliverable

D1.5 Ethical Principles for using Data-Driven Decision in the Cloud (It 1)

Project Acronym:	DUET	
Project title:	Digital Urban European Twins	
Grant Agreement No.	870697	
Website:	www.digitalurbantwins.eu	
Version:	1.0	
Date:	2 June 2021	
Responsible Partner:	GSL	
Contributing Partners:	AIV, IMEC	
Reviewers:	Susie McAleer (21C) Lieven Raes (AIV) Geert Mareels (AIV) Nils Walravens (IMEC) Andrew Stott Yannis Charalabidis	
Dissemination Level:	Public	X
	Confidential – only consortium members and European Commission	

This project has received financial support from the European Union's Horizon 2020 Programme under grant agreement no. 870697

Revision History

Revision	Date	Author	Organization	Description
0.1	10.3.2021	Kletia Noti, Tomas Pavelka, Lieven Raes	GSL, AIV	Initial structure and first draft
0.2	29.4.2021	Tomas Pavelka	GSL	Call for comments on draft principles
0.3	19.5.2021	Kletia Noti, Tomas Pavelka	GSL	Second draft
0.4	25.05.2021	Lieven Raes, Andrew Stott, Geert Mareels	AIV	Edits and review
1.0	02.06.2021	Martina Piantoni, Tomas Pavelka	GSL	Final version

Table of Contents

Executive Summary

The first iteration of this deliverable seeks to (i) discuss the building blocks of the ethical discourse around data-based decision making, and (ii) suggest an ethical code of conduct (ethical principles) for cities in such a context.

For these purposes, this deliverable understands ethics as both the foundational principles of legal norms and the basic guide for their interpretation, but also as ethical norms applicable to situations, which are not specifically regulated by legal rules.

The Introduction in Chapter 1 explains these dynamics by looking at the relationship between legal norms and ethics and how that impacts the ethical discourse in DUET context.

Chapter 2 then sets out a number of preliminary considerations on ethics and the Cloud, which are particularly relevant in the context of disruptive technologies, such as automated data processing systems and AI, HPC, and cloud infrastructure. In order to do that, Chapter 2 follows up directly on deliverables D1.1 (Legal Landscape and Requirements Plan) and D1.2 (Cities Guide to Legal Compliance for Data-Driven Decision Making It. 1) by recalling and updating the main legal requirements and risks in this area, including:

- Privacy - discussing the risks of re-identification, risks of location data resulting in the processing of highly sensitive data, difficulties with obtaining data subject consent and other legal grounds for data processing in a smart city context; and the purpose limitation principle and risks of function creep;
- Cybersecurity - mapping the upcoming legislative change and trends in how to keep data integrity safe, particularly with regard to cloud service providers;
- Cloud infrastructure - discussing the relevant applicable areas of law and other considerations relevant to cloud services, such as even if the conventional models and laws on privacy etc. should apply to cloud as to any other hosting service, there are some specificities of the cloud that may prompt a dedicated legislation;
- HPC and AI - setting out definitions of these concepts and introducing the main legislative action at the EU level concerning these areas (incl. discussing the Commission April 2021 proposal on the Artificial Intelligence Act in more detail).

Chapter 2 then adds supplementary information on the issues of dissemination and publication of data, codes of ethics, trust and trust building for ethical solutions (including the suggestion to introduce peer review mechanisms where there may be lack of regulatory oversight), and some wider societal considerations (with regard to the Commission Green Deal initiative, for example, or freedom of speech).

Chapter 3 sets out the (preliminary) framework for DUET ethical principles (or ethical code of conduct) principally by drawing on the considerations and risks identified by Chapter 2 and previous WP1 deliverables, and based on the exchange of views and experience with other DUET partner organisations.

First, by way of analysis of work-in-progress user defined “epics” of the DUET project, the chapter identifies potential ethical aspects of selected user epics in the way they may deal with data, technology, evidence/data-based decision making, or dissemination and publication of data and results.

Second, the chapter sets out a (non-exhaustive) list of ethical principles, providing a high-level guidance on the following overarching topics:

- Accountability and data sovereignty
- Transparency

- Data quality
- Data quality for publication
- Data security
- Data everywhere
- Transparent and fair use of AI and computer models. Fighting the “opacity” problem.
- Presentation of data or results
- Data ownership and management
- Privacy-by-design
- Anonymised data preference

This present deliverable aimed to spark a broader discussion of ethical issues among DUET partner organisations and inform that discussion by help of selected building stones derived from legal requirements, broader ethical considerations, as well as experience from other projects and other smart city contexts. This ambition was at least in part met judging by the comments we have received from Pilot cities partner organisations and other partners on the draft ethical principles, and suggestions from internal and external reviewers received in the inception and review processes.

The future work on this series of deliverables will involve a continued monitoring of the user defined epics and their practical implementation in the DUET system and its testing, their impact on the (draft) ethical principles and, vice-versa, the impact the formulated ethical principles may have had on these user epics and their implementation. The GSL team will aim to develop the discussion about possible ethical implications of the DUET project among DUET partner organisations more generally.

1. Introduction

This deliverable is the first iteration from the series of two deliverables aiming to provide an ethical code of conduct for cities in data-driven decision making.

This deliverable's scope is nominally restricted to decision-making setups involving the Cloud. Given the dynamic and possibly ambiguous nature of what the Cloud means and involves, however, we seek to adopt a broader understanding of these setups to include, essentially, the use of disruptive technologies (HPC, AI) in combination with the requirement to store and process big data by the help of cloud-based infrastructures. The combination of these resources is what forms the basis of the data-driven and evidence-based decision making of the future.

The deliverable follows up on deliverable D1.1. (Legal Landscape and Requirements Plan). It updates and expands on selected deliverable D1.1's sections, dealing with legal requirements that are considered as the cornerstone of digital "ethics", i.e., privacy and cybersecurity. The deliverable further builds on these to expand the legal requirements and policies regarding the issues specific to the use of disruptive technologies, mainly AI and HPC that are used in the context of data aggregation and the automated and large-scale data processing for decision-making.

Deliverable D1.2 (Cities Guide to Legal Compliance for Data-Driven Decision Making It. 1) sought to set out the areas of the minimum legal requirements to be observed by a smart city solution such as DUET. In that regard, it may be read as a sister-deliverable to the present one, but at the same time smart cities should understand that they cannot hope to implement any fully ethically compliant solutions that would fail to take heed of these legal requirements as well. Therefore, this deliverable may also be seen as expanding on the deliverable D1.2 where it discussed issues of disruptive technologies, such as the legal requirements for automated data processing, or data storage and security issues. These requirements are recapitulated here to the extent they form building blocks for the ethical discourse. Section 3.2 of the deliverable D1.2 also contains a set of working definitions, which will be used throughout this deliverable.

This deliverable seeks to bring a twofold added value:

- First, we take the extra step from the legal requirements (both the applicable law and the law-in-the-making) to see what ethical principles at an abstract level can be ascertained at this stage with regard to the use of disruptive technologies (AI, HPC, Big Data) for a better decision-making (in the Cloud).

- Second, DUET is being built around a set of pre-defined (but still evolving) user defined "epics", which in and of themselves but especially in combination with the robust informational output intended to be achieved by the DUET system can generate ethical conundrums. This series of deliverables will seek to derive ethical questions from these intended use cases and in return attempt to find answers that are applicable to the epics at hand, which also may be transferable to other smart city projects and similar activities. For that purpose, we have requested DUET pilot city organisations for their initial feedback on a draft set of ethical principles (provided in Section 3), and we intend to develop this exchange of views for the second iteration to be published at year three of the project.

This deliverable does not seek to define or redefine what “ethical” means. Instead, it relies on the established corpus of widely available knowledge concerning ethics. However, in its attempt to tackle various ethical questions related to only partially or not at all legally regulated disruptive technologies, the deliverable cannot avoid formulating some views on the boundary between (pure) legal requirements on the one hand, and ethical requirements on the other. There are at least three concurrent principles that shape that boundary and relationship:

1. **Ethical principles provide the foundations for the creation of legal requirements**.
2. **No solution can be considered as “ethical” unless it also meets the applicable (minimum) legal requirements.**[1] In other words, there are limited grounds to argue that a solution which fails to meet the minimum legal requirements should nevertheless be allowed because it serves a particular ethical purpose.
3. **Legal requirements set the minimum standard, while ethics can be more aspirational and seek to impose a higher or the maximum standard.** In other words, just because a solution is legal does not mean that it is the right thing to do.

Another level of differentiation may be observed based on the specificity of legal and ethical standards.

1. **General ethics - specific laws**. Ethics may guide individual actors to do what is right in all aspects of life, while the law may provide rather more specific rules on how to execute such actions.
2. **General laws - specific ethics**. The law may include a wide delegation to individual actors (natural persons, private entities, public authorities) to make a specific decision on an ethical basis. An example of this may be the legal delegation of ethical decision-making to individual practitioners and healthcare services providers by the medical legislation.[2]

This deliverable is structured as follows:

Following this introduction, Section 2 sets out the preliminary and foundational considerations for the discussion of ethical issues around DUET and evidence-based decision-making by smart cities more generally. These partly build on and update (where necessary) information provided by deliverables D1.1 and D1.2 on the applicable legal requirements, but with a particular focus on the overreach of these norms to the ethical realm and specifically with regard to the use of disruptive technologies.

In that logic, sub-Sections such as 2.2 Privacy, 2.3 Cybersecurity or 2.5 HPC and AI – law and ethics of automated and large-scale data processing recall the fundamental principles applicable in these areas, which are foundational for further ethical considerations and for the emerging Section 3. DUET ethical principles.

Sub-Section 2.4 Cloud infrastructure is dedicated for an overview of current trends and initiatives in the area. The fact that legal (and ethical) requirements on Cloud-based services are not yet codified in any significant way makes any discussion of this topic somewhat fragmentary. In that vein, the main applicable legal (and ethical) requirements for cloud-service providers and their users stem from the bundle of other topics discussed in this deliverable (and deliverables D1.1 and D1.2), including mainly privacy and cybersecurity.

[1] This follows from the assumption that at least in the European area, constitutional norms should nowadays guarantee that no laws manifestly in breach of fundamental ethical requirements can be adopted or would survive judicial review. Contrast with historical examples such as the antisemitic and racist Nuremberg Laws of 1935.

[2] The Covid-19 pandemic has raised the public awareness of how the ethical principles-based decision making by healthcare service providers works in practice in the areas of, e.g., patients selection, prioritisation, or re-profilisation of medical resources.

That may be no bad thing, as in general the legal and ethical requirements should relate to assets, intent and risks involved and apply equally whatever technological solution is adopted.

Supplementary sub-Sections (2.6 Dissemination; 2.7 Impact on environment, social justice, distribution of resources, human rights, geopolitics and regional competitiveness; 2.8 Codes of ethics; and 2.9 Trust and trust building for ethical decision-making) add considerations of other factors that may play a role in the design, use and dissemination of the DUET system, as well as similar smart city projects. These complement the foundational framework of Section 2 for the purpose of building the set of ethical principles in Section 3.

Section 3. DUET ethical principles - first version provides, first, an overview of selected work-in-progress use cases (or epics) defined by DUET partner organisations with focus on their (potential) ethical implications for users of different groups. Second, the Section provides a first draft of basic ethical principles intended to (i) inform the pending DUET working streams and design, and (ii) promote the discussion among DUET partner organisations with the view to refine these principles in the forthcoming second iteration of this deliverable.

Section 4. Future work (conclusion) summarizes this deliverable's main findings and sets out the goals for future work.

2. Preliminary considerations on ethics and the Cloud

This section presents some preliminary considerations as building blocks for the ethical framework for evidence-based decision making in the cloud.

2.1 Ethics in the context of disruptive technologies

As explained in the Introduction, there are instances and setups where the guidance of what is the right thing to do cannot be derived simply from the legal requirements. There are cases, where

- the legal norm provides a high-level framework for specific decisions or actions, which then must be guided by ethical considerations, or
- the legal norm provides only a specific rule how to execute a decision or action, but does not give a guidance on when or who should take it, or
- ethics may suggest not infringing boundaries even if there is no legally protected right at stake.

In such scenarios, legal rules may apply only partially (i.e., the legal requirements do not give answer to each and every question related to the decisions or action taken) or do not apply at all. It is in the nature of disruptive technologies to operate in such uncharted territories.

This is particularly the case with disruptive technologies, where the law typically catches on only gradually.

[Tilburg University: Public Sector Data Ethics, From principles to practice[3]]The new data technologies are a formidable and important tool for governance. However, the move from digitising government functions to government relying on the sharing and use of digital data for its functioning brings some entirely new challenges in terms of ethics. Public-sector ethics has traditionally focused on the behaviour of public servants rather than the behaviour of public institutions and departments towards the people.

Luciano Floridi and Mariarosaria Taddeo (2016) defined three components of “data ethics”:

- the ethics of data (how data is generated, recorded and shared);
- the ethics of algorithms (how artificial intelligence, machine learning and robots interpret data)
- the ethics of practices (devising responsible innovation and professional codes to guide this emerging science).[4]

First component, ethics of data, relies more on the legal framework of data that is becoming more precise every day. For example, the GDPR and the related legislation (the ePrivacy Directive) have developed into an overarching system of personal data protection, providing a complete system of remedies.The second and third components of ethical use of data, however, may have posed new challenges to European governments. There are several factors that may be in play:

[3] https://kennisopenbaarbestuur.nl/media/254747/public-sector-data-ethics.pdf

[4] 9 Floridi, L., Taddeo, M. (2016) What is data ethics? Phil. Trans. R. Soc. A 374 (2083), 20160360. DOI: 10.1098/rsta.2016.0360 https://royalsocietypublishing.org/doi/pdf/10.1098/rsta.2016.0360

- bethical codes for governance in some areas had largely developed in the era before big data and do not address the positive or negative ways in which large-scale data, and particularly the use of algorithms, may influence the operation of government. For example, the first proposal for a comprehensive legal framework on AI appeared only in April 2021 in the shape of the European Commission proposal for the Artificial Intelligence Act (see also Section 2.5 HPC and AI – law and ethics of automated and large-scale data processing). That said, the GDPR already introduced some controlling mechanisms for use of automated data processing systems back in 2018.
- Because innovation related to data analysis is not restricted to one sector or operation of government but is becoming something almost every department is expected to engage with, often on an exploratory level where identifying risks is not prioritised. Contact of cities and municipalities with these innovations may require expanding the competences (and training) of responsible officers (e.g., Data Protection Officers), or consider creating even new roles to facilitate responsible and effective use of these innovations by governments.
- The tendency is to rely on the general guidelines provided by data protection law or overarching ethical codes, without creating institutions that can provide day-to-day oversight of projects or audit the way data is being used, particularly at the public-private interface. This is why, in order to boost trust and trust building, this deliverable suggests that there may be room to involve peer-review processes in the areas that are not (yet) subject to regulatory oversight (see also 2.9 Trust and trust building for ethical decision-making). Unlike data protection law, which has become a process that can be closely monitored for compliance (GDPR process of identifying legal basis for data processing, Privacy Impact Assessments, defined roles of the data controller and data processor, etc), ethics of algorithms and other practices pose different types of risks, particularly less apparent ones (e.g. selection bias in the choice of data used, AI embedding bias inherent in the training data - cf facial recognition of non-caucasians). These risks are not so susceptible to process-isation, and therefore may raise various challenges in monitoring and ensuring compliance.

2.2 Privacy

Privacy is considered to be among the main ethical considerations, next to the aims of data integrity sought to be achieved by various (cyber)security measures.[5] To the extent the issue of privacy is about personal data protection, however, the applicable legislation at the EU level and Member State level implementing legislation already provides for an exhaustive system of legal rules and remedies based on the **General Data Protection Regulation (the "GDPR")**.[6]

Deliverables 1.1. (Legal Landscape and Requirements Plan), and 1.2 ((Cities Guide to Legal Compliance for Data-Driven Decision Making It. 1) describe extensively the principal legal requirements in this area and provide guidance on the legal necessities that a smart city should take into account in its decision and policy making processes.

[5] *E.g.,* Hamid Reza Garagardi, "Ethical Considerations in Cloud Computing Systems", MDPI Journal Proceedings 2017, 1, 166.

[6] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

There are several special areas of interest, however, in which smart cities must take into account the existing and developing legal rules as building stones for ethically compliant solutions that rely on disruptive technologies such as AI and HPC and big data processing in the cloud. These include the following concerns:

- risk of re-identification of anonymous data;
- location data revealing sensitive information about data subjects;
- difficulties with obtaining data subjects' consent; and
- data purpose limitation and the danger of function creep.

Thich subsection provides some theoretical background on these concerns, which are then translated to a more specific guidance for smart cities (Section 3. DUET ethical principles).

Risk of re-identification

GDPR does not apply to non-personal data, i.e. data that does not relate to an identifiable natural person (data subject). However, processing of large amounts of data or aggregation of different datasets may significantly increase the risk of data re-identification. A**rticle 29 Working Party's 2014 Opinion on Anonymisation Techniques**[7] identifies the three common risks of re-identification:

1. 'Singling out': the "possibility to isolate some or all records which identify an individual in the dataset."

2. 'Linkability': the "ability to link at least two records concerning the same data subject or a group of data subjects (either in the same database or in two different databases)".

3. 'Inference': the "possibility to deduce, with significant probability, the value of an attribute from the values of other attributes."

Risks under 2 and 3 appear particularly relevant if a smart city system processes large datasets. Where the processing of data results in its re-identification, the GDPR becomes fully applicable to that data(set). The danger is typically in the fact that re-identification happens 'under the radar', resulting in a potential data breach and the unaware data controller being exposed to the risk of penalties for breach of GDPR provisions.

That said, the size of the dataset is not always a clear indicator of re-identification risk. A small dataset could be easier to de-identify because the data subjects are inherently from a small sub-group. The greater risk is a large number of attributes for each data subject, increasing the possibility that a separate set of attributes (e.g. age, geography, occupation, number of children) will identify a separate individual person. In addition, the risk of re-identification may not be spread evenly for the entire dataset - some cases may be identified while others remain anonymous.

The fact that the GDPR may become applicable to a dataset in which the risk of re-identification has materialized does not automatically mean that the organisation handling the data may be penalized for unlawful personal data processing. In such cases, however, it is advisable that the organisation handling the

[7] https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

data takes all reasonable steps, seeks appropriate expert advice and applies all relevant professional standards in order to mitigate the risk of a privacy breach and further unlawful personal data processing.[8]

Location data resulting in the processing of highly sensitive data

Processing of location data, in and of itself but particularly in combination with other data and datasets (such as pictures, names, public registry information), may reveal highly sensitive data such as information on individual's health, political or religious views, or on sexual orientation (see the D1.2 definition of "special categories of data").

Processing of this type of data may raise various ethical issues. DUET consortium members have provided examples from their countries of origins. For instance, there may be systems introduced to counter terorism or improve road safety, but which can be used for purposes they were not intended for and without any information to the citizens about this new use. E.g., in the city of Antwerp, CCTV cameras have been installed near synagogues originally for security purposes, but of which cases are known that they have been used also to catch individuals who visit the synagogue in breach of the Covid-19 restrictions. Similarly, ANPR cameras data can be misused to see what individuals are frequenting gay bars or abortion centers. Even if these misuses amount to an infringement of the applicable legislation and may therefore be penalized (i.e., GDPR's legal requirements are at stake), these examples also raise ethical questions that may be left unaddressed by the legislation. For instance, should such systems be put in place if their misuse for illegitimate purposes cannot be prevented?

Difficulties with obtaining data subjects' consent; other grounds for lawful data processing

It may be difficult or practically impossible to obtain data subjects' consent in a smart city context. This is particularly difficult in cases of large-scale data processing, or when processing data from sensors for the purposes of statistical counting and similar. The D1.1 and D1.2 deliverables explain the pitfalls of doing this.

However, it should be recalled that subjects' consent is not the only legal basis for lawful personal data processing under the GDPR:

- processing is necessary for compliance with a legal obligation to which the controller is subject (Art. 6(1)(c) of the GDPR);
- processing is necessary in order to protect the vital interests of the data subject or of another natural person (Art. 6(1)(d) of the GDPR);
- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (Art. 6(1)(d) of the GDPR).

Therefore, in a smart city context, instead of attempting to collect data subjects' consent, a public authority may also rely on these other grounds to lawfully collect and process citizen data for the stated purposes based on the power (or obligation) conferred by applicable law. Where no such laws exist, public authorities are typically stakeholders, which may initiate legislative action or actively participate in existing legislative procedures (at local, state, or even international levels). Indeed, it may be an ethical question in itself whether a public authority should be obliged to use all means at its disposal to seek legislative change that would empower it to lawfully collect and process personal data for legitimate interests and public good.

[8] See, for example, the Eurostat Manual on Disclosure Control Methods (1996), available at https://ec.europa.eu/eurostat/ramon/statmanuals/files/manual_on_disclosure_control_methods_1996.pdf

Data subjects' consent typically serves a dual purpose. One is to ensure privacy in the narrow sense (i.e., keeping private information and data that a subject does not wish to become public), another one is the data subjects' consent with the type of data processing to which he/she is being subjected to. This has specific implications under the GDPR when it comes to automated data processing for example. Such protection is further expanded in cases of the AI use - see Section 2.5 HPC and AI – law and ethics of automated and large-scale data processing).

Furthermore, in a broader ethical sense, a valid consent by data subjects-citizens may be effective in the ethical or even in the political sense as a consent to (consciously) take part in the wider issues concerning their polis. The rules on privacy in the automated processing/AI context may even be understood to require such broader citizenship awareness and active participation.

The applicable or future legislation may ease the requirements for collecting valid data subject consent, but these will likely be limited to narrowly defined exemptions. For example, the proposed ePrivacy Regulation seeks to allow a non-consent based processing of users' equipment-emitted information such as in provision of physical movements' tracking services (e.g.,services enabling statistical people counting in a specific area), but subject to further safeguards to minimise impact on individuals' privacy.[9]

In summary, smart cities should seek to obtain citizens' consent where this is practically possible and, in general, should aim to maximise the transparency on how they collect, process and publish citizen data. For further detail, see Section 3. DUET ethical principles.

The purpose limitation principle under the GDPR and risk of function creep in the event of data re-use

When consent to process personal data is given for a specific purpose under the GDPR (as it always needs to be), any processing beyond that purpose may be unlawful unless additional consent with the processing for the new purpose is obtained. Similarly, legal bases other than consent (as provided by the GDPR) typically also allow processing of personal data only for defined purposes, for example for the objectives and purposes set out by the legislation empowering public authorities to collect certain citizen data.

Adhering to such purpose limitation principle helps to avoid the phenomenon of "function creep", which broadly means using data for a different purpose than it was originally collected for, or which is not in line with the legal basis used for the original data collection, or covered by the data subject's consent.

This applies equally to situations where the original legal basis for data processing is not consent but other legal ground (such as the performance of tasks entrusted to public authorities by law), but where the new or additional purpose for processing of such data cannot be based on such legal basis or exceeds the purpose limitation principle.

Finally, there may be examples of situations in which the purpose for data processing may appear as broadly within the original purpose (e.g., combating crime), but where a re-use of the data may still raise ethical questions. Consider the following recent example from Belgium: ANPR cameras have been installed at the Flemish seaside for the purpose of detecting and preventing major criminal activity. However, during the Covid-19 lockdown in 2020, the authorities resorted to using these cameras to detect people travelling to

[9] March 2020 ePrivacy Regulation proposal.

their seaside apartments, potentially in breach of then applicable administrative restrictions.[10] In addition, the enforcement authorities or even the legislator may have a leeway in how to define or interpret the original purpose or an objective of certain measures. DUET external reviewers pointed us to an example from the UK, where the notion of “serious crime” is legally defined broadly as “anything you can be arrested for”, whereas the public perception of what a serious crime is may be much more narrow (limited to grave felonies such as murder, violent robbery, human or drug trafficing, etc.). Such mismatches can result in citizens’ misunderstanding of the law enforcement’s objectives when deploying surveillance measures, for example, and undermine their legitimate expectations more broadly speaking. We expand on this fundamental transparency principle in Section 3. DUET ethical principles.

2.3 Cybersecurity

Cybersecurity risks are an increasing phenomenon and smart city systems may be particularly vulnerable or particularly attractive as targets. The Duet infrastructure is not immune to these risks, as well. Risks are thought of as a formula of vulnerability times threat, times consequence. Vulnerabilities are weaknesses in a system which give rise to specific risks when combined with a threat.

Due to the Covid pandemic, in a single month, the world became quickly digitally connected — and vulnerable to cybersecurity risks — than ever. In March 2020, organizations that had forever required employees to gather at a common physical location were suddenly using the Internet to facilitate remote interaction among a vast constellation of home offices. This encompassed various fields of the economy, including financial institutions, businesses relying on digital services and so on.

Deliverable D1.1 laid out the main regulatory framework for ensuring cybersecurity of systems across the board:

- **Regulation 2019/881 on ENISA and ICT Cybersecurity Certification (Cybersecurity Act)**: the Regulation lays down a framework for the establishment of European cybersecurity certification schemes for the purpose of ensuring an adequate level of cybersecurity for ICT products, ICT services and ICT processes in the Union, as well as for the purpose of avoiding the fragmentation of the internal market with regard to cybersecurity certification schemes in the Union.
- The **Directive 2016/1148 on security of network and information systems (NIS Directive)**: The Directive aims at ensuring a level playing field across Member States which guarantees a high common level of security of network and information systems across the EU in the context of the Digital Single market. The directive explained the relative measures that should be taken by the EU Member States in order to reach the goals of the directive.

Due to the Covid-19 pandemic, in a single month, the world became quickly digitally connected — and vulnerable — than ever. In March 2020, organizations that had forever required employees to gather at a common physical location were suddenly using the Internet to facilitate remote interaction among a vast constellation of home offices. This encompassed various fields of the economy, including financial institutions, businesses relying on digital services and so on.

The new political guidelines for the new European Commission 2019-2024 laid down that cybersecurity remains a priority area for further action in the years to come. To implement the European Commission Recommendation adopted in March 2019 to ensure a high level of cybersecurity of 5G networks across the

[10] https://www.datapanik.org/2021/03/13/in-de-vlaamse-centrumsteden-komen-er-in-sneltempo-bewakingscameras-bij-mede-dankzij-corona/

EU, on 29 January 2020, the Commission published the 5G toolkit prepared by the NIS cooperation group with cybersecurity mitigating measures. On 17 February 2020 it presented it to the ITRE committee. Later on, the Council decision of 14 May 2020 extended until 18 May 2021 the restrictive measures framework against attacks which threaten the EU or its Member States given the rise in malicious activities and cyberattacks during the pandemic.

On 16 December 2020, the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy presented a new EU Cybersecurity Strategy. Such a strategy aims at bolstering Europe's collective resilience against cyber threats and ensuring that all citizens and businesses can fully benefit from trustworthy and reliable services and digital tools. In the strategy the Commission presented two proposals: a Directive on measures for high common level of cybersecurity across the Union (see related wagon 'NIS 2') as well as a new Directive on the resilience of critical entities. On Monday 22 March 2021, the European Council adopted its conclusions on the cybersecurity strategy with the work of the coming years: Among others the design of a network of operational centers (SoC) and the common cyber unit, the finalization of the 5G toolbox, the establishment of security standards, the defense of strong encryption (yet allowing access by law enforcement), strengthening both the cyber diplomacy toolbox planning its own action plan.

The European Commission considered that the 2016 NIS directive suffers from several weaknesses and initiated its revision in December 2010. These are the main changes likely to be introduced with the NIS 2:

- Add new sectors based on their criticality for the economy and society, and by introducing a clear size cap – meaning that all medium and large companies in selected sectors will be included in the scope.
- Eliminates the distinction between operators of essential services and digital service providers. Entities would be classified based on their importance and divided respectively in essential and important categories with the consequence of being subjected to different supervisory regimes.
- The proposal imposes a risk management approach providing a minimum list of basic security elements that must be applied. The proposal introduces more precise provisions on the process for incident reporting, content of the reports and timelines.
- The proposal strengthens supply chain cybersecurity for key information and communication technologies. Member States in cooperation with the Commission and ENISA, will carry out coordinated risk assessments of critical supply chains.

Computer security incident response teams (CSIRTs) designated by the Member States will have the task to promote the adoption and use of common or standardised practices, classification schemes and taxonomies in relation to:

- incident handling procedures;
- cybersecurity crisis management;
- coordinated vulnerability disclosure.

Chapter IV of the directive will provide rules on risk management and reporting that can interest DUET in the framework on how to react in case of cybersecurity breach.

This proposed directive aims to emphasise the importance of cloud computing systems, and their security. The following requirements may be applicable to clouds:

- higher security standards.

- stronger form of international cooperation.
- One Member State jurisdiction. In order to take account of the cross-border nature of the services and operations of DNS[11] service providers, TLD[12] name registries, content delivery network providers, cloud computing service providers, data centre service providers and digital providers, only one Member State should have jurisdiction over these entities. Jurisdiction should be attributed to the Member State in which the respective entity has its main establishment in the Union, meaning the place where the decisions related to the cybersecurity risk management measures are taken in the Union (typically the place of the companies' central administration in the Union). If such decisions are not taken in the Union, the main establishment should be deemed to be in the Member States where the entity has an establishment with the highest number of employees in the Union. The criterion of establishment for the purposes of this Directive implies the effective exercise of activity through stable arrangements, regardless their legal form or whether the network and information systems are physically located in a given place[13].

The new directive will be subject to negotiations between the co-legislators, notably the Council of the EU and the European Parliament. Once it is agreed, the EU Member States will have 18 months to transpose it.

2.4 Cloud infrastructure

Legal requirements applicable to the cloud are mostly uncodified. In order to build and provide, or use, a cloud-based service, there is a bundle of interplaying legal requirements. These include issues discussed in other sections of this deliverable, and deliverables D1.1 and D1.2: privacy, cybersecurity, non-personal data flow (data portability), liability, etc.

An analysis of the requirements for cloud solutions based on the business models of Urban Digital Twins is discussed in a DUET deliverable D2.4 (Cloud Based Business Models Analysis). We would refer Cities to that deliverable for more information about cloud-based infrastructure issues.

The following points summarize the main themes, including ethical and legal, in the current discussion of cloud infrastructure at the EU level:

- Joint investment in cross-border cloud infrastructures and services to build the next generation cloud supply;
- **European marketplaces for cloud services**, where users will have a single portal to cloud offerings meeting key EU standards and rules;
- **EU Cloud Rulebook** for cloud services, which will provide a single European framework of rules, transparency on their compliance and best practices for cloud use in Europe;
- **Edge computing** (expectation that in the next few years, about 80% of data will be processed by smart devices closer to the user)
- Cloud computing and edge computing will contribute to achieving the sustainability goals of the **European Green Deal** in areas such as farming, mobility, buildings and manufacturing;
- The **Regulation on the free flow of non-personal data** should raise legal certainty for cloud users by ensuring the free movement of all data in the EU

[11] DNS means domain name systems

[12] TLD means top-level-domain

[13] See Recital 64 of the proposal. Available at: https://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/com/2020/0823/COM_COM(2020)0823_EN.pdf.

- **Data portability**: the free flow of non-personal data Regulation also builds trust through facilitating a self-regulatory work on cloud switching and cloud security.
- ENISA is working on a **single European cybersecurity certification scheme** for cloud services. The scheme will provide increased assurance to businesses, public administrations and citizens that their data is secure wherever they are stored or processed.
- **European mapping of data flows**: Monitoring data flows across the European Union's territory is of strategic importance to EU decision-making and investment choices in the area of cloud computing.
- **Standardised cloud service level agreements**: that should guarantee an high level of quality of Cloud services in the European market.

Cloud service providers are, on the whole, subject to the cybersecurity requirements described in Section 2.2 Cybersecurity above, and legal requirements for ensuring privacy, confidentiality, and integrity of the stored data (these are extensively discussed by Deliverables D1.1 and D1.2). For the purposes of this deliverable, the main takeaway should be that smart cities use only trusted Cloud service providers, which guarantee to comply strictly with the set legal requirements.

Even though we believe that cloud infrastructure should, in general, be subject to the same laws and ethics requirements as any other hosting solution (in order not to yield to some relaxation of the achieved standards), it is true that some characteristics may be specific to cloud infrastructures that may raise difficulties if the conventional models and regulation is applied. For example, the data controller (the user of the cloud storage service to store and process its data in the cloud) may not have rights to audit or inspect the (cloud) data processor. Or the data controller may not even know in which country the data is being physically stored or how many copies exist, due to the overlap of various transmission/conduit, caching and hosting functions. Such characteristics may prompt the need to legislate on cloud infrastructures more specifically. We plan to expand on these issues in the future iterations of this deliverable, as well as in a deliverable dedicated specifically to cloud infrastructures (D1.7, Recommendations for European Cloud Infrastructure).

Smart cities would therefore be advised to follow closely such future legislative actions, as well as the Commission's initiatives concerning the single European cybersecurity certification scheme, and seek to include in their contracts with cloud service providers the standardised cloud service level agreement clauses, which may facilitate legal compliance on all sides. Such a solution can also be expected to meet the required ethical standard for a state-of-art use of cloud-based services.

Data portability

The EU has already adopted legislative measures to facilitate the portability of data between various data processors across EU Member States. This includes personal data (the free movement of personal data is governed by the GDPR) and non-personal data. The non-personal data portability is primarily ensured by the Regulation on a framework for the free flow of non-personal data in the European Union[14] For purposes of this deliverable's consideration of cloud infrastructures, it is worth recalling the regulation's main objectives:

- Free movement of non-personal data across borders: every organisation should be able to store and process data anywhere in the European Union
- The availability of data for regulatory control: public authorities will retain access to data, also when it is located in another Member State or when it is stored or processed in the cloud

[14] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union.

- Full consistency and synergies with the cybersecurity package, and clarification that any security requirements that already apply to businesses storing and processing data will continue to do so when they store or process data across borders in the EU or in the cloud.
- Easier switching of cloud service providers for professional users. The Commission has started facilitating self-regulation in this area, encouraging providers to develop codes of conduct regarding the conditions under which users can port data between cloud service providers and back into their own IT environments

The EU legislation in the area has already spurred a number of working groups (e.g. on cloud switching, or cloud security.[15] It is advisable for smart cities as frequent consumers of cloud storage and computing services to monitor these sources closely.

2.5 HPC and AI – law and ethics of automated and large-scale data processing

High Performance Computing (HPC)

HPC refers to computing services with super high computational power that have the possibility to solve complex problems.

The European Commission recognises [source] that HPC plays a crucial role in several fundamental sectors:

- Society: HPC applications are a strategic resource to understand our ever-changing world, and transform global challenges into innovation opportunities for growth and jobs. It is vital in the context of cybersecurity to increase the security of our digital systems;
- Industry: the use of HPC applications over the cloud will make it easier for SMEs without the financial means to invest in in-house skills to develop and produce better products and services.

HPC is a fundamental part of the European Data Strategy. The European High-Performance Computing Joint Undertaking (EuroHPC Joint Undertaking) was established in 2018. EuroHPC JU is pooling European resources to buy and deploy top-of-the-range supercomputers and develop innovative exascale supercomputing technologies and applications. It aims to improve quality of life, advance science, boost industrial competitiveness, and ensure Europe’s technological autonomy.

In addition, the European Commission announced a new program for HPC that has led to the adoption of a new regulation in this field.[16] Its main goals are:

- develop, deploy, extend and maintain a world-class exascale and post-exascale HPC and data infrastructure, driven by key scientific, industrial and social applications
- federate high-performance and quantum computing resources and make them accessible to users across Europe

[15] https://ec.europa.eu/digital-single-market/en/news/cloud-stakeholder-working-groups-start-their-work-cloud-switching-and-cloud-security.

[16] COUNCIL REGULATION (EU) 2018/1488 of 28 September 2018 establishing the European High Performance Computing Joint Undertaking.

- develop technologies and applications to underpin a competitive supercomputing ecosystem, develop greener computing and exploit the synergies of HPC with AI, big data and cloud technologies.
- provide secure cloud-based HPC services for a range of public and private users, including for the European public data space, as presented in the 2020 European Data Strategy

AI can be used to drive complex HPC simulations, making them faster, more accurate and self-improving. Equally, HPC can be used to explain, understand and improve the decisions made by AI. The European Commission has noted the close convergence between HPC and AI.[17]

Automated decision-making and Artificial Intelligence (AI)

Even though the DUET project has not yet identified any AI related use cases in the stricter understanding of the term “AI” (machine learning or self-learning systems), this deliverable seeks to understand AI more broadly as covering also automated decision making setups, or algorithms for processing data used for decision or policy making. This is because many issues typical for AI in the narrow sense (black box / opacity problem, accountability, human agent issue, bias) are likely to be relevant for many automated decision making settings as well.

In the words of the Commission High-level Expert Group on Artificial Intelligence, it is necessary to “*develop, deploy and use AI systems in a way that adheres to the ethical principles of: respect for human autonomy, prevention of harm, fairness and explicability. Acknowledge and address the potential tensions between these principles “*[18] More unpacked, the High-level Expert Group explains that these principles encompass:

- ***The principle of respect for human autonomy****: The allocation of functions between humans and AI systems should be human-centric design and leave meaningful opportunity for human choice. This means securing human oversight over work processes in AI systems. AI should support humans in the working environment and aim for the creation of meaningful work.*
- ***The principle of prevention of harm:*** *AI systems should neither cause nor exacerbate harm or otherwise adversely affect human beings. This entails the protection of human dignity as well as mental and physical integrity. AI systems and the environments in which they operate must be safe and secure.*
- ***The principle of fairness:*** *the use of Automated decision systems should never lead to people being deceived or unjustifiably impaired in their freedom of choice.*
- ***The principle of explicability:*** *this means that processes need to be transparent, the capabilities and purpose of AI systems openly communicated, and decisions explainable to those directly and indirectly affected. Without such information, a decision cannot be duly contested. An explanation as to why a model has generated a particular output or decision (and what combination of input factors contributed to that) is not always possible. These cases are referred to as ‘black box’ algorithms and require special attention. In those circumstances, other explicability measures such as traceability, auditability and transparent communication on system capabilities may be required, provided that the system as a whole respects fundamental rights. The degree to which explicability is needed is highly dependent on the context and the severity of the consequences if that output is erroneous or otherwise inaccurate.*

[17] COMMISSION STAFF WORKING DOCUMENT Equipping Europe for world-class High Performance Computing in the next decade. Accompanying the document Proposal for a Council Regulation on Establishing the European High Performance Computing Joint Undertaking (18 September 2020), page 29.
[18] High-Level Expert Group on Artificial Intelligence, “ETHICS GUIDELINES FOR TRUSTWORTHY AI” (2018), page 2.

Section 4.3 of Deliverable D1.1 has sketched some legal and ethical aspects of AI systems. In [add date], the European Commission [announced] that it will propose a regulation proposal in the first quarter of 2021, which will aim to safeguard fundamental EU values and rights and user safety by obliging high-risk AI systems to meet mandatory requirements related to their trustworthiness (discussed further in 2.11 Trust and trust building for ethical decision-making).

There are several important interactions between the AI (understood broadly as automated data processing) and the GDPR. The GDPR applies to the processing of personal data wholly or partly by automated means. The GDPR uses several different formulations to refer to decisions and processing that involve automation. Article 2 states that the GDPR "*applies to the processing of personal data wholly or partly by automated means*"; Articles 21 and 22 refer to "*automated individual decision-making*" in their titles. Article 22 prohibits "*decision based solely on automated processing, including profiling*." Recital 71 maintains this terminology, applying to decisions based "*solely on automated processing*", which data subjects have a general right to not be subjected to, and "*automated decision-making and profiling based on special categories of personal data*" which are only allowed in limited circumstances. When automated decisions are allowed under the contract or consent exceptions set out in Article 22, data controllers are required to implement specific safeguards. Article 22 in conjunction with 13(f) of GDPR also requires that data controllers must provide the data subjects with information necessary to ensure fair and transparent processing, which discloses: *"the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject*.

The Commission's proposal on the Artificial Intelligence Act

On 21 April 2021, the European Commission released a Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act).[19] The proposal follows the European Commission's White Paper on AI, adopted in 2020.[20]

This is the first ever proposed legal framework on AI, which seeks to comprehensively address its risks. It may position the EU to play a leading role globally, thus fostering its role to help shape global norms and standards and promote trustworthy AI that is consistent with Union values and interests. We consider, therefore, that discussing this proposal in more detail may add a significant value for the purposes of this deliverable, and for the emerging set of ethical guidelines that will need to be followed in the context of increasingly automated data processing systems.

In the Preamble, the Commission clarifies that the promotion of AI-driven innovation is closely linked to the Data Governance Act[21], the Open Data Directive[22] as well as other initiatives under the EU strategy for data[23] , which are aimed at establishing trusted mechanisms and services for the re-use, sharing and pooling of data that are essential for the development of data-driven AI models of high quality.

[19] European Commission, 21 April, 2021, Proposal for a Regulation laying down harmonised rules on artificial intelligence, COM(2021) 206 final, available at: https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence-artificial-intelligence.

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

[21] Proposal for a Regulation on European data governance (Data Governance Act) COM/2020/767.

[22] Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information, PE/28/2019/REV/1, OJ L 172, 26.6.2019, p. 56–83.D.1.1.

[23] Commission Communication, A European strategy for data COM/2020/66 final.

Definition of AI

Under Article 1 of the Proposed Regulation, an ‘artificial intelligence system’ (AI system) means software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with.

Personal scope: to whom the rules will be addressed

The following actors will be subject to the Regulation’s provisions:

- providers placing on the market or putting into service AI systems in the EU (irrespective of whether they are established in the EU or in a third country (i.e., outside of the EU);
- users of AI systems established within the EU, under whose authority and responsibility the AI system is used; as well as
- EU institutions, offices, bodies, and agencies when they are providers or users of AI systems.

It is possible that both the organisations responsible for DUET administration and the DUET system as such may come under the scope of the Regulation, insofar they can be either a “provider” and/or a “user”.

The Regulation has extraterritorial effect: namely, actors (providers and users) established in a third country are also subject to the Proposed Regulation to the extent the AI systems affect persons located in the EU. This is similar to the GDPR, which has had an impact on the worldwide development of data protection regulation.

Subject-matter scope: the prohibited practices

Article 5 of the Proposed Regulation prohibits certain AI practices that are considered a clear threat to the safety, livelihoods, and rights of people, including:

- AI systems that manipulate human behaviour, opinions or decisions through choice architectures or other elements of a user interface;
- Exploiting information or prediction about an individual or group of individuals to target their vulnerabilities or special circumstances.
- These practices will be in scope where they result in a person to behave or take a decision to their detriment, i.e. concern behaviour that causes or is likely to cause that person or another person physical or psychological harm.
- AI systems that evaluate or classify the trustworthiness of natural persons based on their social behaviour or known or predicted personal or personality characteristics, leading to detrimental or unfavourable treatment.
- The use of ‘real-time’ remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement. There may be certain exceptions to this prohibition, including for law enforcement purposes.
- AI systems used for indiscriminate surveillance applied in a generalised manner to all natural persons without differentiation. This may include the monitoring or tracking of individuals through direct interception or gaining access to communication, location, meta data or other personal data collected in a physical or virtual environment where it is performed on a large-scale.

It is observed that a similar approach is also followed at national level. For example, in France, the bill on bioethics[24] prohibits medical decisions solely taken on the basis of AI treatment (i.e. algorithmic processing used for preventive, diagnostic or therapeutic acts, which is learned from massive data) and requires that a “human guarantee” is given. Similarly, the revised Law on data processing[25] reiterates that "no decision that produces legal effects with respect to a person or that significantly affects him/her may be adopted on the sole basis of automated processing of data of a personal nature, including profiling". However, "the aforementioned prohibition does not apply in the case of individual administrative decisions adopted” in specific circumstances.

Subject-matter scope: high risk AI systems

Certain AI systems will be considered high-risk as regards their potential risk of harm to health and safety or adverse impact on fundamental rights. Types of such systems are defined in annexes to the Proposed Regulation, and include typically systems that are intended to be used as safety components of a product or are themselves a product.[26] The European Commission may update the annexes following a prescribed risk assessment procedure.

These AI systems will be subject to stricter requirements provided by the Proposed Regulation, such as the duty to establish a risk management system, duty to test the systems and to observe certain obligations when training the AI systems on data and the data governance, technical documentation and record-keeping, transparency, human oversight, accuracy, robustness and cybersecurity (in more detail below).

Indeed, one of the main concerns with AI systems identified early on[27] is the so-called black box effect in which the algorithm that governs decisions made by the systems is unknown to its users or to the addressees. In this respect, Article 9 of the Proposed Regulation provides that “*High-risk AI systems shall be designed and developed so as to ensure that their outputs can be verified and traced back throughout the high-risk AI system’s lifecycle, notably through the setting up of features allowing the automatic generation of logs*”.

The Proposed Regulation sets out detailed conditions that providers of high-risk AI systems must comply with:

- use detailed and specific risk management systems and subject the system to a conformity assessment;
- only use high quality data that does not incorporate intentional or unintentional biases and is representative, free from errors and complete;

[24] French bill, Projet de loi nº 3833/2021, Article 11 (“Supporting the dissemination of scientific and technological progress in accordance with ethical principles”).

[25] French Law No 493/2018, Article 21 amending Law No 17/1978.

[26] These include: AI systems used to dispatch or establish priority in the dispatching of emergency first response services; AI systems used to determine the access to education or vocational training; AI systems during the recruitment, promotion, or termination process; AI systems that evaluate the creditworthiness of persons; AI systems used by public authorities to evaluate the eligibility for public assistance benefits and services; AI systems used in a law enforcement context to prevent, investigate, detect, or prosecute a criminal offence or adopt measures impacting on the personal freedom of an individual or to predict the occurrence of crimes or events of social unrest with a view to allocate resources devoted to the patrolling and surveillance of the territory; AI systems used for immigration and border control, including to verify the authenticity of travel documentation and to examine asylum and visa applications; and AI systems intended to be used to assist judges at court.

[27] High-Level Expert Group on Artificial Intelligence, “ETHICS GUIDELINES FOR TRUSTWORTHY AI” (2018).

- conduct post-market monitoring of the operation of the system and notify any serious incident or malfunctioning to the relevant national regulator;
- register the system on a public register;
- keep records and logs, and be transparent to users about the use and operation of the system;
- ensure human oversight through appropriate technical and/or organizational measures; and
- ensure the robustness, accuracy, and security of the AI system.

We consider that these obligations may also provide helpful guidance for the design of other automated decision-making systems, and we therefore advise that these are reasonably taken into account for the emerging DUET ethical principles (see Section 3. DUET ethical principles).

The obligations for the users of high-risk systems are more limited. Users must ensure that technology is in accordance with the instructions for use and take appropriate technical and organisational measures to address risks created by the system. Users must also monitor the operation of the system and keep records of the description of the data used.

The Proposed Regulation further imposes specific obligations upon (i) authorised representatives of providers, (ii) importers, (iii) distributors of high-risk AI systems and (iv) other third parties involved in the AI value chain.

Sanctions

Non-compliance with the rules laid down in the Proposed Regulation can give rise to GDPR-inspired administrative fines up to EUR 20,000,000. In the case of an undertaking, these fines are up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher. National supervisory authorities shall be competent for monitoring and enforcing compliance. A **European Artificial Intelligence Board** (EAIB), composed of representatives of the national supervisory authorities, a representative of the European Data Protection Supervisor (EDPS) and a representative from the European Commission, shall be established. The EAIB's main task will be to supervise the consistent application of the Proposed Regulation.

Other issues

It is worth mentioning that the Proposed Regulation aims at establishing an EU database of high-risk AI systems, which will collect a set of mandatory information from providers of such systems. The European Commission will control and operate that database.

The Proposed Regulation aims also at establishing a dedicated European Artificial Intelligence Board (EAIB) to help assist and advise the European Commission in relation to the subject matter of the regulation.

2.6 Dissemination

In November 2020, the European Commission published a proposal for a new regulation on European data governance (the Data Governance Act).[28] We expect that this legislation, if adopted, may have a major impact on the legal framework for data sharing. This regulation proposes a model based on the neutrality and transparency of data intermediaries, which are organisers of data sharing or pooling, to increase trust among

[28] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on European data governance (Data Governance Act) COM/2020/767 final

stakeholders. To ensure its neutrality, the data-sharing intermediary cannot deal in the data on its own account and will have to comply with strict requirements. The proposed regulation envisages:

- Several measures to **increase trust in data sharing**, as the lack of trust is currently a major obstacle and results in high costs.
- Creation of new **EU rules on neutrality** to allow novel data intermediaries to function as trustworthy organisers of data sharing.
- Measures to **facilitate the reuse of certain data held by the public sector**. For example, the reuse of health data could advance research to find cures for rare or chronic diseases.
- Means to **give European citizens control** on the use of the data they generate, by making it easier and safer for companies and individuals to voluntarily make their data available for the wider common good and under clear conditions.

Article 2 of the proposed regulation provides a definition of data sharing: *"'data sharing means the provision by a data holder of data to a data user for the purpose of joint or individual use of the shared data, based on voluntary agreements, directly or through an intermediary".* Chapter 3 of the proposed regulation, titled requirements applicable to data sharing services, aims at introducing a notification procedure in order for an entity to be able to provide data sharing services. The proposed regulation seeks also to establish a new authority, the **European Data Innovation Board**, entrusted with the following tasks:

- to facilitate the cooperation between national competent authorities under this Regulation through capacity-building and the exchange of information, in particular by establishing methods for the efficient exchange of information relating to the notification procedure for data sharing service providers and the registration and monitoring of recognised data altruism organisations.
- to advise the Commission on the prioritisation of cross-sector standards to be used and developed for data use and cross-sector data sharing, cross-sectoral comparison, and exchange of best practices with regards to sectoral requirements for security, access procedures, while taking into account sector-specific standardisations activities.
- to advise and assist the Commission in developing a consistent practice of the competent authorities in the application of requirements applicable to data sharing providers.

Smart cities would be advised to follow these developments closely, as they may significantly change the approach to public sector information and information sharing between public authorities and also between businesses / citizens on the one hand, and public administration on the other hand. The currently applicable public sector information legislation has been extensively discussed by deliverable D1.1 (Legal Landscape and Requirements Plan).

2.7 Wider societal considerations

AI and robotics technologies require considerable computing power, which comes with an energy cost. Can we sustain massive growth in AI from an energetic point of view when we are faced with unprecedented climate change? As regards the use of resources we should underline that technological devices are made by materials that already damage the environment. Increasing the production and consumption of technological devices such as robots will exacerbate this waste problem, particularly as the devices will likely be designed with 'inbuilt obsolescence.

AI technology, particularly machine learning, will require more and more data to be processed. And that requires huge amounts of energy. According to Strubell, Ganesh, and McCallum (2019), the carbon footprint of training, tuning, and experimenting with a natural language processing AI is over seven times that of an average human in one year, and roughly 1.5 times the carbon footprint of an average car, including fuel, across its entire lifetime. Those issues are crucial especially in this period in which for the climate changing situation and the excessive level of pollution the World governments are approving plans for the next thirty years to prevent Ambiental catastrophe.

From the social point of view automated decision systems do not only impact the environment. In the previous section we underlined what is the impact on human people. Here we will focus on how automated decision systems could impact human rights. Below there are several examples:

- **Surveillance**: 'Networks of interconnected cameras provide constant surveillance over many metropolitan cities. In the near future, vision-based drones, robots and wearable cameras may expand this surveillance to rural locations and one's own home, places of worship, and even locations where privacy is considered sacrosanct, such as bathrooms and changing rooms. As the applications of robots and wearable cameras expand into our homes and begin to capture and record all aspects of daily living, we begin to approach a world in which all, even bystanders, are being constantly observed by various cameras wherever they go' (Wagner, 2018).
- **The Internet of Things**. A myriad of connected home devices, including appliances and televisions, nowadays regularly collect data that may be used as evidence or accessed by hackers. Video can be used for a variety of exceedingly intrusive purposes, such as detecting or characterising a person's emotions. AI may also be used to monitor and predict potential troublemakers. In China, there are examples of face recognition used not only to identify individuals, but to identify their moods and states of attention both in re-education camps and ordinary schools.
- **Freedom of speech**: Freedom of speech and expression is a fundamental right in democratic societies, and it could be profoundly affected by AI. AI is regarded by technology companies as a solution to problems such as hate speech, violent extremism, and digital misinformation, we can see it also today since Facebook is using his algorithms to remove the fake news around Covid-19. This use of artificial intelligence was already experimented by India; where sentiment analysis tools are increasingly deployed to gauge the tone and nature of speech online and are often trained to carry out automated content removal. The Indian Government has also expressed interest in using AI to identify fake news and boost India's image on social media. Automated content removal risks censorship of legitimate speech; this risk is made more pronounced by the fact that it is performed by private companies (in this context we can see the erasure of Trump's Facebook and twitter profiles), sometimes acting on the instruction of the government. Heavy surveillance affects freedom of expression, as it encourages self-censorship.

2.8 Codes of ethics

The EU institutions seek to involve stakeholders in creating dedicated codes of ethics for the use of AI and automated decision systems. The initiative has an ambition to develop codes of ethics not only for public authorities but also for private companies (which may be far more advanced and experienced in the use of AI systems). Consider the following principles suggested by the private sector.

- AI products should reflect "Invented for life" ethos, which combines a quest for innovation with a sense of social responsibility.

- AI decisions that affect people should not be made without a human arbiter. Instead, AI should be a tool for people.
- We want to develop safe, robust, and explainable AI products.
- Trust is one of our company's fundamental values. We want to develop trustworthy AI products. (we will explain more in detail trustworthy artificial intelligence in the next section)

Several approaches may be implemented:

- "Human-in-command" (HIC): In this approach, the AI product is used purely as a tool. At all times, people decide when and how to use the results presented by the tool. An example is when a machine helps people with classification tasks.
- "Human-in-the-loop" (HITL): In this approach, people can directly influence or change decisions made by an AI product.
- "Human-on-the-loop" (HOTL): This approach concerns those cases in which the parameters relevant for decisions are defined by people during the design process, but the decisions themselves are delegated to the AI product. The application allows those affected by the decision to appeal for review. This ensures that people not only define the parameters for decision making beforehand, but also check retrospectively whether the decision was carried out in the intended sense.

As noted above, the French legislation offers an example of a similar approach, based on the "human guarantee" principle.

2.9 Trust and trust building for ethical decision-making

High-Level Expert Group on Artificial Intelligence observed that in creating trustworthy artificial intelligence systems, different groups of stakeholders have different roles to play:

- Developers should implement and apply the requirements to design and development processes;
- Deployers should ensure that the systems they use and the products and services they offer meet the requirements
- End-users and the broader society should be informed about these requirements and able to request that they are upheld.[29]

The Group adds the following non-exhaustive list of requirements:

- **Human agency and oversight** Including fundamental rights, human agency and human oversight
- **Technical robustness and safety** Including resilience to attack and security, fall back plan and general safety, accuracy, reliability and reproducibility
- **Privacy and data governance** Including respect for privacy, quality and integrity of data, and access to data
- **Transparency** Including traceability, explainability and communication
- **Diversity, non-discrimination and fairness** Including the avoidance of unfair bias, accessibility and universal design, and stakeholder participation
- **Societal and environmental wellbeing** Including sustainability and environmental friendliness, social impact, society and democracy

[29] High-Level Expert Group on Artificial Intelligence, "ETHICS GUIDELINES FOR TRUSTWORTHY AI" (2018), page 14.

- **Accountability** Including auditability, minimisation and reporting of negative impact, trade-offs and redress

Peer-review mechanisms

Until ethical standards / rules become law, the standard legal system oversight mechanisms, such as judiciary or public enforcement agencies cannot typically intervene if something goes wrong. In other cases, law cannot intervene because there is no-one with sufficient legal standing to invoke the legal remedies (e.g., large groups) or where there is no tangible loss or concrete harm to values protected by legal norms.

For some such cases, societies have set up various frameworks and institutions that use a peer-review system to decide whether a particular action is or is not state-of-art. Where law does not regulate particular details of certain matters, e.g., in pharmaceutical regulation requires an ethical committee to oversee clinical trial procedures for compliance with the ethical standards (as well as higher-level legal standards). These ethical committees or institutions are typically composed of experts in the area.

We consider that to the extent disruptive technologies are only partially or not at all regulated, it could be considered whether (i) ethical oversight mechanisms that already exist could apply to the area, or, if they do not exist or are underdeveloped, (ii) whether their creation should be proposed and where we can draw inspiration.

3. DUET ethical principles - first version

This first version of an ethical framework is grounded in selected use cases identified by pilot city organisations, and in turn seeks to provide these organisations with some ethical guidance as well as derive lessons potentially applicable to any interested smart city organisations with similar ambitions.

User types

First, it may be useful to set out various user types identified for use cases by the pilot city organisations.[30] This is because the applicable ethical considerations (and legal requirements) are likely to differ between these. For example, a citizen user of a publicly available version of DUET will typically not have legal or factual access to sensitive or confidential data, but, on the other hand, may use the data and models made available for any possible legitime purpose. Conversely, a DUET admin or a public servant with direct access to the DUET system will have access to various restricted data types, but will be constrained as to the purposes for which he/she may use them.

The following overview sorts user types into overarching categories and attributes to them some characteristics and potential use cases identified thus far by the DUET partner organisations. These use cases have been selected with regard to their likely impact on ethical considerations from the work-in-progress document on user epics https://docs.google.com/spreadsheets/d/1L9o91u0_dBgCVOlesBwN1tsJmpMtssbQjd_XXmJDdEc/edit#gid=0

DUET administrator (system administrator)

Characteristics:

- Connecting data sources
- Restricting access to data sources
- Designing visualisation and presentation features

Selected epics:

- (**G15**) I want to be able to connect data sources so I can be sure that the necessary data and information is available
- (**G16**) I want to be able to restrict the access to data sources so I can be sure confidential data is not made publicly available

Likely ethical considerations:

- Accountability and transparency - knowing and making known the origin of the data, respecting and passing on data limitations
- Data quality
- Data security
- Transparent and fair use of data models
- Privacy-by-design and confidentiality, risks of re-identification of anonymous data
- Setting results presentations technical options (colour modes, visualisations, diagrams, etc.)

[30] We have relied on a number of DUET work in progress documents, which may be published as separate deliverables.

Public servant / city official / city employee / urban planner (a public authority)

Characteristics:

- Access to data, models and results
- Setting the purpose of data processing
- Making evidence/data-based decisions
- Position to negotiate with partners (public, private) access to or sharing of data

Selected epics:

- (**G2, G3**) I can discover the causes of pollution. I can assess the impact of changes to the local situation on the traffic in my area of interest / the impact on citizens well-being in the city.
- (**P1**) I want to see all existing attributes for buildings and objects in 3D representation of the city
- (**Pilsen**) I want to connect existing data resources of the city to the digital twin and make sure they are up-to-date, interoperable, and include all available attributes, with the goal to make my daily work more efficient thanks to working with different data sources in a single environment

Likely ethical considerations:

- Finding the best data for the purpose
- Understanding the possibility of selection bias in the choice of data and what is “best”
- Do I understand the data models? Am I able to interpret their results? Am I able to use the system?
- Transparency towards citizens that their data is used, decisions made based on data concerning them
- Ensuring data is of sufficient quality to be published
- Balancing the interests between law enforcement and keeping data separate (issue of purpose).
- Asking / requesting third parties to provide data

Policy maker (a public authority)

Characteristics:

- Access to data, models and results
- Purpose of data processing
- Making data available as open data
- Balancing of public and private interests

Selected epics:

- (**P8**) I want to make the 3D data of the city available as open data (see data section for already opened data). The city balances the relevance of opening the data with policy objectives, the price, the relevant level of granularity and so on.
- (**P6**) I want to motivate investors of major development projects to provide 3D data during the building planning and permission process

Likely ethical considerations:

- Finding the best data for the purpose
- Understanding the possibility of selection bias in the choice of data and what is “best”
- Do I understand the data models? Am I able to interpret their results? Am I able to use the system?
- Transparency towards citizens that their data is used, decisions made based on data concerning them
- Ensuring data is of sufficient quality to be published
- Asking / requesting third parties to provide data

Investor (a private party)

Characteristics:

- Restricted / no access to confidential information
- Business to public information sharing

Selected epics:

- (**P7**) I want to provide 3D data (as well as BIM data) of my envisaged major construction project to the city, thus allowing the city administration to assess my project in 3D, so I can inform citizens about my project in the official digital twin of the city (under the 'future' view).

Likely ethical considerations:

- Ensuring data is of sufficient quality to be shared
- How can the data be further (re-)used

Registered user who can upload data (a private party)

Characteristics:

- Private to public information sharing

Likely ethical considerations:

- Ensuring data is of sufficient quality to be shared
- How can the data be further (re-)used

Citizen (a private party)

Characteristics:

- Restricted / no access to confidential information. Broad definition of confidential (incl. personal data, trade secrets, restricted use based on license information).

Selected epics:

- (**G6**) I can inspect the current traffic density.
- (**G7, G8**) I can inspect the current level of pollution.
- (**G9-G11**) I can inspect historical information.
- (**G13**, **G14**) I can provide municipalities with some data that I collect.
- (**Flanders**) I want to have an idea about the mobility flows in my city and neighbourhood.

Likely ethical considerations:

- How is my / my co-citizens' data processed?
- For what purposes?
- Is the data safe?
- Are any automated processes involved in the decision-making about me / using my data?
- Do I trust my city? Is the city transparent about its decisions and policies, and data management?

The draft ethical principles

Second, we have prepared a draft set of ethical principles for broader consideration among the DUET partner organisations and sought to attract comments from the pilot city organisations in April/May 2021. The first draft of these principles was derived from the following sources:

- Primary desk research scoping similar activities by smart cities elsewhere in the EU and overseas;[31]
- Discussions with DUET partners (AIV and IMEC) and external reviewers;
- Extrapolation from more detailed or, conversely, high level, legal requirements and principles.

In order to attract more detailed comments from pilot city organisations, we provided an (unexhaustive) list of broadly framed questions in order to illustrate what type of ethical considerations they should take into account. These are the questions we asked:

- *"I had been assigned a task and I was not sure whether I am allowed to use the data collected by my City for this purpose."*

- *I was not sure whether my City has data available that would help me to complete a particular task. I was unsure who to turn to to find out."*

- *"I felt that I lacked the skills and knowledge in data analytics / visualisation in order to use the available data to make a data-based decision."*

- *"I had to rely on a result given by a data processing model to carry out a task or make a decision, but I was not sure whether the result was reliable."*

- *"I wanted to use a data processing model but I was not sure that I understood fully how it works."*

- *"When working with some data (e.g. noise, pollution), I realised that the data reveal the source or the cause of these externalities (e.g., the exact location of a polluter). I was wondering if someone may be responsible for committing an administrative offence (or even a crime) and I was not sure whom to contact about this. I was not sure whether I could make this data public, and what the reaction from the general public might be.*

- *"I worked with anonymous data but after combining different data sources, they began to reveal information about identifiable persons (personal data)."*

- *"I was working with a third-party provided dataset, but realized that these are actually personal, highly sensitive data (e.g., data showing individual people's health condition, or data allowing me to learn about a person what his/her religion or sexual orientation is). I wasn't sure about whom to contact and what to do with the database."*

- *"We cooperated with a private organisation (a firm, company, non-profit) on a joint task. The private organisation planned to collect some data in the course of the task. I was not sure whether the organisation could share the data with us. I was not sure how to ask that organisation to share the data with us. The organisation refused to share the data with us and I didn't know what to do."*

[31] These include, e.g., the City of Barcelona Digital Standards (https://www.barcelona.cat/digitalstandards/en/init/0.1/index.html); the Smart Flanders Open Data Charter (https://smart.flanders.be/open-data-charter/); the Toronto Quayside project (https://waterfrontoronto.ca/nbe/portal/waterfront/Home/waterfronthome/projects/quayside).

- *"I wanted to present some data with help of visualisation but the system won't allow me to choose the colour I want or a type of visualisation that would work best in my opinion."*

After evaluation of the comments received, the following text sets out the first version of ethical principles that might, subject to further discussion and evaluation, contribute to a more definitive guidance that could be followed by DUET partner organisations in their development and execution of the DUET project, as well as other stakeholders and smart cities with similar ambitions.

1. Accountability and data sovereignty

1.1. Know the origin of the data, its lawful and ethical uses, and any limitations on their sharing or publication.

2. Transparency

2.1. You should know what data you collect and for what purposes.

2.2. The data subjects (e.g. the citizens) should know what data you collect about them and for what purposes.

2.3. Be transparent about the scope and source of the data, as well as the limitations of the data. Explain what information the data contains, how (and where) it was collected, whether it is static data, updated regularly, or real-time.

2.4. If the data is publicly available, provide a link to the data repository/source url.

2.5. Make sure that decision makers are aware of the deficiencies / limitations of the data.

3. Data quality

3.1. Get the best data as you can for your purposes. Best may mean:

3.1.1. data most suited for your purpose;
3.1.2. most complete, correct, and up-to-date data (clean data);
3.1.3. data with a transparent track record of their collection, storage, and the log of previous processing;
3.1.4. data with a clear licence to (further) use.

3.2. Take active steps to ensure and maximise the quality, objectivity, usefulness, integrity and security of data.

4. Data quality for publication

4.1. If the data is sufficient for an internal use (within the services of the city), it is typically equally good for making the data publicly accessible (open).

4.2. Use open standards and open licenses.

4.3. Publish data only after you have cleared the applicable legal requirements.

5. Data security

5.1. The integrity and security of data should be maximised.

5.2. Use trusted third-party services providers (e.g., approved by the future European Union Cybersecurity Certification Scheme on Cloud Services (EUCS)).

6. Data everywhere

6.1. Promote the use of data in public interest, be active in seeking out data that may be (re)used in public interest.

6.2. Actively explore the ways in which data can be obtained from partners (private or public) with whom you engaged in a joint activity (e.g., public procurement).

7. Transparent and fair use of AI and computer models. Fighting the “opacity” problem.

7.1. Cities should strive to develop the officials’ ability to understand, interpret and use automated decision-making systems. They should understand at least the basics of the underlying algorithms and the data used. This can be achieved by a targeted education and training, for example.

7.2. Data subjects (citizens) should be informed about the fact that automated decisions are being taken about them and with the help of their data. To the extent possible, cities should strive to make sure that data subjects also understand the underlying algorithms, to the extent practicable.

7.3. Algorithms and automated decisions should be fair and proportional. They should not prejudice the data subjects. Even though some bias may be inherent in data, the algorithms and the data they use (or train on) should not create or perpetuate material biases (racial, ethnical, sexual, political, religious, etc.)

7.4. Ensure an element of human control over the AI:

7.4.1. Individuals to whom human oversight is assigned should fully understand the capacities and limitations of the AI system and should be able to duly monitor its operation, so that signs of anomalies, dysfunctions and unexpected performance can be detected and addressed as soon as possible.

7.4.2. Data subjects should be granted the right to appeal relating to data processing and the automated decisions that affect them.

8. Presentation of data or results

8.1. The way data or data-based decisions are presented should avoid creating or perpetuating bias (e.g., the use of red and green color coding for visualisations).

9. Data ownership and management

9.1. Data ownership typically goes hand in hand with the responsibility for data management.

9.2. Third parties contracted out for city data management should be chosen responsibly, adequate data processing agreements should be put in place.

10. Privacy-by-design

10.1. Comply with all legal requirements when acquiring, using, or publishing personal data. (see also D1.2 Cities Guide to Legal Compliance for Data-Driven Decision Making).

10.2. If you come across a personal data breach, report to your Data Protection Officer.

11. Anonymised data preference

11.1. Do not use personal data unless it is strictly necessary for your task and proportionate to meeting the pre-defined purpose of your activity.

11.2. If anonymous data is not available, but personal data is, ensure that the data is anonymised before its further use, if possible.

11.3. Non-anonymised data should in no case be made public (or open data), unless strictly required for carrying out the task in question, and unless cleared by the Data Protection Officer for publication.

11.4. Where data is anonymised, do not proactively take any steps in the direction to re-identify the data (link the data to individual persons). The following techniques and procedures, for example, should be avoided unless the goal is actually to re-identify otherwise anonymous or pseudonymised data:

11.4.1. *Singling out*, which corresponds to the possibility to isolate some or all records which identify an individual in the dataset;

11.4.2. *Linkability*, which is the ability to link, at least, two records concerning the same data subject or a group of data subjects (either in the same database or in two different databases). If an attacker can establish (e.g. by means of correlation analysis) that two records are assigned to a same group of individuals but cannot single out individuals in this group, the technique provides resistance against “singling out” but not against linkability; or

11.4.3. *Inference*, which is the possibility to deduce, with significant probability, the value of an attribute from the values of a set of other attributes.

11.5. If the risk of re-identification materializes on a given dataset, take all reasonable steps, seek appropriate expert advice and apply all relevant professional standards in order to mitigate the risk of a privacy breach and further unlawful personal data processing.

4. Future work (conclusion)

This present deliverable aimed to spark a broader discussion of ethical issues among DUET partner organisations and to inform that discussion by help of selected building stones derived from legal requirements, broader ethical considerations, as well as experience from other projects and other smart city contexts.

We trust that this ambition was at least partially met judging by the comments we received from Pilot cities partner organisations and other partners on the draft ethical principles, and suggestions from internal and external reviewers received in the inception and review processes. We aim to develop and broaden that exchange of views going forward.

This first version of ethical principles may, however, be found lacking in several ways:

a) The list of ethical principles may be under-inclusive as regards issues specific to disruptive technologies and data management processes used by the smart city stakeholders. Even though we tried to avoid that by means of soliciting pilot city partners' views on the draft principles, the list may also be over-inclusive as regards certain concepts not encountered by smart cities in practice.

b) The draft ethical principles may need further discussion among DUET partner organisations insofar they may have a steering effect on a number of DUET's current and planned activities.

c) DUET user defined epics are an ongoing work-in-progress, so the first version of these principles may be found too abstract to give helpful advice to the pilot city partner organisations or other DUET partners.

d) The visual and systematic side of the draft principles may need to be improved in order to convey the message across more effectively.

The future work on this series of deliverables will involve addressing these issues especially by way of a continued monitoring of the user defined epics and their practical implementation in the DUET system and its testing, their impact on the (draft) ethical principles and, vice-versa, the impact the formulated ethical principles may have had on these user epics and their implementation. The GSL team will aim to develop the discussion about possible ethical implications of the DUET project among DUET partner organisations more generally.