MASTER THESIS

Data and the City

And Just Like That, Everything became Personal

LL.M. International Technology Law Program

at

the [redacted]

[redacted]

Master: International Technology Law

Wordcount: 19690

Supervisor: Silvia De Conca

Second Reader: Mark Leiser

DATA AND THE CITY

And Just Like That, Everything became Personal

A research on the concept of personal data, Article 4(1) GDPR, and its application and interpretation in the smart city

[redacted]

Master's thesis submitted in partial fulfilment of the requirements for the Degree of
Master of Laws
in
International Technology Law

“*Regulators having to regulate emerging technologies face a double-bind problem: the effects of new technology cannot be easily predicted until the technology is extensively deployed. Yet once deployed they become entrenched and are then difficult to chang*e.”

—

David Collingridge, ‘The Social Control of Technology’ (1980)

Abstract

This Master's thesis aims to explore the key challenges and implications for the protection of personal data in the context of smart cities and proposes measures to ensure sustainable and effective data protection in this environment. The thesis critically analyses the interpretation and application of Article 4(1) of the General Data Protection Regulation (GDPR) in the context of smart cities and identifies a disconnection between the GDPR's technology and industry-neutral framework and the socio-technical constructs of smart cities. The thesis argues that relying solely on the nature of data to protect personal data is not sufficient and proposes a risk-based approach to data protection that focuses on potential risks and harms caused by data processing. The thesis also emphasises the need for a holistic approach to data management, with a focus on adaptability and flexibility to accommodate emerging technologies. The thesis concludes that updating the GDPR's definition of personal data to reflect smart environments and initiating discussions on red lines for data use can ensure sustainable protection in light of other data-driven technologies. Overall, the thesis offers insights into the challenges and opportunities for data protection in the context of smart cities and proposes a novel approach to address the complex issues at hand.

Table of Contents

List of Abbreviations

AI	Artificial Intelligence
CJEU	Court of Justice of the European Union
DA	Data Act
DGA	Data Governance Act
EC	European Commission
ECHR	European Convention on Human Rights
EDPS	European Data Protection Supervisor
EDPB	European Data Protection Board
EU	European Union
GDPR	General Data Protection Regulation
ICT	Information Communication Technology
OECD	Organisation for Economic Co-operation and Development
SLL	Stratumseind Living Lab
WP29	Article 29 Data Protection Working Party

Chapter I.

Introduction

1.1. Problem Statement

In a world where digital technologies have become ubiquitous, data has emerged as the fundamental building block of our globalised society.[1] The smart city is a product of this trend, where interconnected devices rely on data to operate seamlessly.[2] With the proliferation of data in smart cities, there has been a surge of investment in data-driven smart technologies that aim to enhance performance, improve efficiency, and generate unprecedented amounts of data.[3] The implementation and advancement of cutting-edge technologies such as the Internet of Things (IoT) and Artificial Intelligence (AI) are fundamental to the global expansion of smart cities.[4] The advancement of the smart city is characterised by the sophisticated data processing technologies that gather data with the objective of enhancing urban life.[5] The increasing volume and value of data processed creates challenges to the principles of data protection laws, particularly in regards to the concept of personal data.[6] The inescapable presence of personal data in the era of data-driven technologies highlights the importance of understanding the boundaries of the concept of personal data.[7] Smart cities can reveal information about individuals and lead to new risks in the domain of personal data protection.[8] Datasets may not initially include personal data but can still pose a threat to individuals' rights due to the potential repurposing of data for

[1] Hajduk, P. (2021). The Powers of the Supervisory Body in the GDPR as Basis for Shaping the Practices of Personal Data Processing. *Review of European and Comparative Law (RECoL)*, 45, 57-76; Solove, D. J., & Hartzog, W. (2021). *Breached!*. Oxford University Press.

[2] Quach, S., Thaichon, P., Martin, K. D., Weaven, S., & Palmatier, R. W. (2022). Digital technologies: Tensions in privacy and data. *Journal of the Academy of Marketing Science*, *50*(6), 1299-1323.

[3] Dalla Corte, L. (2020). Safeguarding Data Protection in an Open Data World: On the idea of balancing open data and data protection in the development, 14.

[4] Stefanouli, M., & Economou, C. (2018). Data protection in smart cities: Application of the EU GDPR. In *Conference on Sustainable Urban Mobility* (pp. 748-755). Springer, Cham.

[5] Kaluarachchi, Y. (2022). Implementing data-driven smart city applications for future cities. *Smart Cities*, *5*(2), 455-474.

[6] Saglam, R. B., Nurse, J. R., & Hodges, D. (2022). Personal information: Perceptions, types and evolution. *Journal of Information Security and Applications*, *66*, 103163.

[7] Denker, A. (2021). Protection of Privacy and Personal Data in the Big Data Environment of Smart Cities.*The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences, XLVI-4/W5-2021*, 181-186.

[8] Gellert, R. (2021). Personal data's ever-expanding scope in smart environments and possible path(s) for regulating emerging digital technologies. *International Data Privacy Law*, 11(2), 196–208.

unintended uses, known as function creep.[9] The changing nature of personal data in a smart society presents challenges in ensuring that data is collected, stored, and used in a way that is consistent with data protection laws, jeopardising the core values of data protection.[10] This affects the traditional notions of value attribution, making data protection applicable to nearly anyone and to any information at any time.[11] As the characteristics of these smart-systems follow an 'everything is information' method, advanced data-driven technologies and the ubiquitous availability of information make the nature and interpretation of personal data a rather elusive concept.[12] As a result, the definition and interpretation of personal data is constantly evolving in the context of smart environments, leading to a growing recognition of an ever-expanding scope in smart environments and data protection becoming, indeed, 'the law of everything'.[13]

The 'datafication' of everyday life has elevated the significance of safeguarding personal information for the European Union.[14] The General Data Protection Regulation (GDPR) is widely recognized as a crucial framework for the digital domain not only in the Europe Union but also beyond. However, the concept of personal data and the applicability of the GDPR to new technologies are still being explored.[15] The concept of personal data has been a topic of debate among legal scholars for a long time, but its importance has only increased with the rise of novel data-driven technologies and capabilities.[16] The current definition of personal data, as envisaged in Article 4(1) of the GDPR, has

[9] Function creep refers to the situation where data to the corresponding applications are gradually used differently than they originally were intended to be used. *See* Koops, B. J. (2021). The concept of function cree*p. Law, Innovation and Technology, 13(1), 29-56.*

[10] Finck, M., & Pallas, F. (2020). They who must not be identified—Distinguishing personal from non-personal data under the GDPR. *International Data Privacy Law, 10*(1), 11–36. *See also* Dalla Corte, L. (2019). Scoping personal data: towards a nuanced interpretation of the material scope of EU data protection law. *European Journal of Law and Technology,* 10(1).

[11] Purtova, N. (2018). The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, *10*(1), 40-81.

[12] Dalla Corte, L. (2022). Personal Data in the EU Legal System. In *Elgar Encyclopaedia of Law and Data Science* (pp. 259-267). Edward Elgar. *See also* Elliot, M., O'hara, K., Raab, C., O'Keefe, C. M., Mackey, E., Dibben, C., ... & McCullagh, K. (2018). Functional anonymisation: Personal data and the data environment. *Computer Law & Security Review*, *34*(2), 204-221.

[13] Gellert, R. (2021). Personal data's ever-expanding scope in smart environments and possible path(s) for regulating emerging digital technologies. *International Data Privacy Law*, 11(2), 196–208.

[14] Finck, M., & Pallas, F. (2020). They who must not be identified—Distinguishing personal from non-personal data under the GDPR. *International Data Privacy Law, 10*(1), 11–36. *See also* Gstrein, O. J., & Ritsema van Eck, G. J. (2018). Mobile devices as stigmatizing security sensors: The GDPR and a future of crowdsourced 'broken windows.' *International Data Privacy Law, 8*(1), 80–81; Søe, S. O. (2021). Non-natural Personal Information. Accounting for Misleading and Non-misleading Personal Information. *Philosophy & Technology*.

[15] Mildebrath, H. (2022). Understanding EU data protection policy. *European Parliamentary Research Service*. https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/698898/EPRS_BRI(2022)698898_EN.pdf

[16] Among others, *see* Dalla Corte, L. (2019). Scoping personal data: towards a nuanced interpretation of the material scope of EU data protection law. *European Journal of Law and Technology,* 10(1); Dalla Corte, L. (2020). Safeguarding Data Protection in an Open Data World: On the idea of balancing open data and data protection in the development, 14; Denker, A. (2021). Protection of Privacy and Personal Data in the Big Data Environment of Smart Cities.*The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences, XLVI-4/W5-2021*, 181-186; Finck, M., & Pallas, F. (2020). They who must not be

come under scrutiny due to the challenges posed by smart cities to the protection of personal data.[17] The interpretation of the concept of personal data has been judged to be problematic.[18] Much of the literature has focused on the issue of identification and when an individual is identifiable from information,[19] but there has been limited exploration on the concept of personal data itself and how it is related to the individual in light of the permeation of data-driven technologies.[20] By exploring the technological aspects of smart environments and the interaction between digital developments and the urban environment, the thesis will seek to clarify what qualifies as personal data in smart cities and the necessary nexus between an individual and the information. The aim of this thesis is to critically examine and critique the current definition of personal data, as it relates to the challenges posed by smart cities, and to suggest possible solutions for ensuring the protection of personal data in the context of smart cities. This thesis will provide a comprehensive analysis of the legal framework surrounding personal data and will consider the various perspectives of a number of legal scholars, as well as the practical implications of the interpretation of personal data in the context of smart cities. Moreover, this thesis aims to address the gap in the literature on the concept of personal data and its relationship to the individual in the age of datafication.[21] Given the significance of safeguarding personal data in such an age, comprehending the precise meaning of 'personal data' has become more important than ever.[22]

1.2. Research Questions and Significance

The research aims to examine the interpretation and application of the term 'personal data' as defined in Article 4(1) of the GDPR in the context of data-driven technologies in smart cities. The main objective is to determine if the current definition of personal data is suitable and sustainable in light of the

identified—Distinguishing personal from non-personal data under the GDPR. *International Data Privacy Law, 10*(1), 11–36; Gellert, R. (2021). Personal data's ever-expanding scope in smart environments and possible path(s) for regulating emerging digital technologies. *International Data Privacy Law*, 11(2), 196–208; Koops, B. J. (2014). The trouble with European data protection law. *International data privacy law*, *4*(4), 250-261; Purtova, N. (2018). The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, *10*(1), 40-81.

[17] Gellert, R. (2021). Personal data's ever-expanding scope in smart environments and possible path(s) for regulating emerging digital technologies. *International Data Privacy Law*, 11(2), 196–208

[18] Hallinan, D. & Gellert, R.M. (2020). The Concept of 'Information'. An Invisible Problem in the GDPR. Script-Ed, 17 (2), 269-319; Koops, B. J. (2014). The trouble with European data protection law. *International data privacy law*, *4*(4), 258; Purtova, N. (2018). The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, *10*(1), 40-81.

[19] Finck, M., & Pallas, F. (2020). They who must not be identified—Distinguishing personal from non-personal data under the GDPR. *International Data Privacy Law, 10*(1), 11–36

[20] Denker, A. (2021). Protection of Privacy and Personal Data in the Big Data Environment of Smart Cities. *The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences, XLVI-4/W5-2021*, 181-186.

[21] Wong, B. (2019). Delimiting the concept of personal data after the GDPR. *Legal Studies*, *39*(3), 517-532.

[22] Søe, S. O., Jørgensen, R. F., & Mai, J. E. (2021). What is the 'personal' in 'personal information'?. *Ethics and Information Technology*, *23*(4), 625-633.

challenges posed by these technologies, and if the GDPR can meet its objectives of protecting individuals' fundamental rights and freedoms.[23]

The significance of personal data protection is rooted in the fact that it is a fundamental right in EU law.[24] European Data Protection law is acknowledged as the 'gold standard' for data protection laws, including its definition of personal data.[25] As the use of smart technologies and the creation of smart cities become more prevalent,[26] it is essential to examine whether smart cities are subject to data protection regulations under the GDPR, and if citizens of smart cities can avail themselves of their right to personal data protection.[27] The study aims to contribute to the discussion on the definition of personal data by exploring its relevance within a data protection framework that is rapidly globalising and where data-focused technologies are continuously evolving.[28] Despite the scholarly attention to data protection law and technological advancements, the concept of personal data in the context of smart city environments has not been extensively studied.[29] In addition, the research will analyse how personal information has evolved and how it is perceived differently due to advancements in technology.[30] It aims to reconcile the growing demand for data in smart environments with the protection of personal data. The results of this research will be essential in guiding policymakers and stakeholders in developing suitable and sustainable data protection regulations that ensure the protection of individuals' fundamental rights and freedoms in the face of technological advancements. The research aspires to contribute to the understanding of personal information and how it has been impacted by technology, by answering the following research question:

"To what extent is the current interpretation and application of 'personal data', Article 4(1) of the GDPR, suitable and sustainable in light of the permeation of other data-driven technologies, such as smart cities?"

[23] As stated in Article 2 of the GDPR, the regulation only applies to the processing of 'personal data'.

[24] Zhao, B., & Chen, W. (2019). Data protection as a fundamental right: The European General Data Protection Regulation and its exterritorial application in China. *US-China Law Review*, 16, 97, 99.

[25] Omotubora, A., & Basu, S. (2020). Next generation privacy. *Information & Communications Technology Law*, *29*(2), 151-173.

[26] Galič, M. (2019). Surveillance, privacy and public space in the Stratumseind Living Lab: The smart city debate, beyond data. *Ars Aequi, special issue July/August*.

[27] European Union Agency for Fundamental Rights and Council of Europe (2018). Handbook on European data protection law. *Fra.europa.eu*. Retrieved from https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf

[28] Gellert, R. (2021). Personal data's ever-expanding scope in smart environments and possible path(s) for regulating emerging digital technologies. *International Data Privacy Law*, 11(2), 196–208.

[29] Saglam, R. B., Nurse, J. R., & Hodges, D. (2022). Personal information: Perceptions, types and evolution. *Journal of Information Security and Applications*, *66*, 103163.

[30] Saglam, R. B., Nurse, J. R., & Hodges, D. (2022). Personal information: Perceptions, types and evolution. *Journal of Information Security and Applications*, *66*, 103163.

The sub-questions that help answer this research question are:

1. *What is the current interpretation of personal data as envisaged in Article 4(1) of the GDPR by European case law and bodies, and how has this interpretation evolved over time?*
2. *What are smart cities and what are the specific challenges to the concept of personal data as envisaged in Article 4(1) of the GDPR posed by smart cities for the protection of personal data rights?*
3. *How does the implementation of the concept of personal data as envisaged in Article 4(1) of the GDPR in smart cities impact the protection of personal data rights, and what can be done to ensure that this protection is maintained in the face of the increasing data processing in smart environments?*

.

1.3. Legal Framework

The core of this research will be based on the concept of personal data, embedded in European Data Protection law. The General Data Protection Regulation in particular with Article 4(1) of the GDPR forms the core of the analysis. 'Data' that is not personal data will be referred to as non-personal data. Moreover, distinguishing exactly what is implied by 'personal data' and by 'non-personal data will be discussed in chapter 2.5.

1.4. Research Methodology

The methodology of this thesis will be based on a comprehensive analysis of the current European legal framework on the concept of personal data, which is central to European Data Protection law. The analysis will be based on Article 4(1) of the GDPR, which provides the foundation for the interpretation and application of the concept of personal data in European data protection law. The thesis will examine the formulation of the GDPR and Article 4(1) and analyse EU law, doctrine, and jurisprudence as the primary sources of information. European case law of the European Court of Justice will be used to provide a comprehensive definition of personal data in EU data protection. In order to achieve the objectives, EU laws, as well as their legislative history and legal interpretation, are examined. This will be complemented by analysis of interpretations by scholarship, other European authoritative and legal bodies to identify trends and patterns in the interpretation of personal data and the protection of personal data rights in the context of increasing data processing in smart cities. All the foregoing will form a conclusion on the formulation of the concept.

In order to provide a comprehensive analysis, this research will employ a legal dogmatic methodology that enables an examination and analysis of the GDPR to determine how the law is, or de *lege lata.*[31] Academic journal articles will be reviewed for insights into the regulation of emerging technologies and their application to the GDPR and data protection law. The role of technology in data protection and the applicability of personal data, especially in relation to smart environments, will also be examined. The aim of the research is to understand the rationale behind the definition of personal data and analyse the debates and critiques surrounding data protection law and the GDPR. The objective of this research is to contribute to the development of a comprehensive and coherent legal framework for personal data protection in smart cities, that takes into account the challenges posed by the increasing amounts of information being processed in these environments, and the need to safeguard the fundamental rights of individuals. The thesis will explore the idea that data protection is becoming the law of everything and further develop it by analysing alternative organising notions for personal data in the context of smart environments.[32]

1.5. Overview of Chapters

This thesis focuses on the application of the concept of personal data in the context of smart cities. The body of the thesis will consist of five chapters, each of which will have its own set of subsections.

Chapter I. The first chapter of the thesis serves as an introduction to the topic significance and relevant legal framework as well as significant terms and issues.

The second chapter will answer the first sub-question outlining the legal concept of personal data in the EU.

Chapter II. This chapter evolves around material scope of Article 4(1) as defined in the GDPR and delves into the concept of personal data and the different elements of the definition as interpreted under EU law.

Subsequently, chapters three, four, and five aim to answer the second sub-question.

Chapter III. The third chapter provides an overview of the concept of smart city, accompanied by a practical demonstration through the Stratumseind Living Lab, which serves as a real-world example of a smart city.

Chapter IV. The fourth chapter applies the concept of personal data to the context of smart cities and examines the implications of data protection in this environment.

[31] Vranken, J. (2012). Exciting times for legal scholarship. *Law and method*, *2*(2), 42-62.

[32] Purtova, N. (2018). The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, *10*(1), 40-81.

Chapter V. The fifth chapter builds upon the preceding chapters. This chapter will identify the areas in which the GDPR is challenged by smart environments and the limitations posed by current legislation.

Penultimately, in chapter six the third sub-question will be answered.
Chapter VI. The sixth chapter offers solutions and recommendations for ensuring the protection of personal data in smart cities.

Chapter VII. The seventh and final chapter concludes the thesis by giving a review of the findings and a substantial response to the research question will be provided.

The concept of personal data under the GDPR will be illuminated from a technological workable perspective analysing its digital presence. This thesis will researches the notion of personal data 'in action', by better understanding information and its relationship to people and solutions for the challenges of tomorrow. However, not losing sight of the fact, that law in the books does not always become, nor does it always resemble, law in action.[33]

[33] Koops, B. J. (2014). The trouble with European data protection law. *International data privacy law*, *4*(4), 258.

Chapter II.

On the Concept of Personal Data: Article 4(1) of the General Data Protection Regulation

2.1. European Data Protection Law and The General Data Protection Regulation

The European Union is a pioneer in data protection and has a long history of safeguarding personal data.[34] In the 1970s, some EU Member States introduced laws to regulate the processing of personal information by corporations and public institutions.[35] This was in response to the increasing amount of data being collected and processed by these entities.[36] The European Convention on Human Rights (ECHR) recognizes the importance of personal information protection as a fundamental aspect of private and family life, as outlined in Article 8 ECHR.[37] The Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data in 1981, also known as Convention 108, expands upon the right to privacy as defined in Article 8 ECHR and has laid the

[34] Van Der Sloot, B. & & Zuiderveen Borgesius, F. J. (n.d.). The Eu General Data Protection Regulation: A New Global Standard For Information Privacy [*Working draft*]. Retrieved from https://bartvandersloot.com/onewebmedia/SSRN-id3162987.pdf

[35] The German state of Hesse passed the first data protection law in 1970. This was only applicable in the state. In 1973, the first national data protection law was passed in Sweden. By the late 1980s, several other European countries (France, Germany, the Netherlands and the United Kingdom) had also adopted data protection legislation. *See* European Union Agency for Fundamental Rights (2018). Chapter 2: Data protection terminology (pp. 21). In *Handbook on European Data Protection Law*.

[36] Hondius, F. W. (1975). *Emerging data protection in Europe*. Amsterdam: North-Holland Publishing Company; New York: American Elsevier Publishing Company.

[37] The ECHR guarantees the right to respect for private and family life, home and correspondence, and any interference by public authorities must be lawful, justified by a legitimate public interest, and necessary for a democratic society. *See* Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights) (ECHR), Article 8.

foundation for the development of data protection laws in Europe.[38] This Convention is the first international binding instrument on data protection.[39]

In light of the fast-paced technological advancements, the EU adopted comprehensive data protection laws specifically tailored to the digital age.[40] In particular, the European Union has established the General Data Protection Regulation (GDPR) as the cornerstone of its data protection framework. The GDPR replaced the Data Protection Directive and has since become the foundation of EU data protection law. The Regulation became applicable on May 25, 2018, and has a far-reaching impact, not only within the European Union but also globally.[41] The GDPR sets out a comprehensive set of rules and regulations for the protection of personal data, and aims to harmonise data protection laws across the European Union.[42] The regulation places an emphasis on privacy rights, ensuring that individuals have control over their personal data, and that organisations are held accountable for its protection.[43]

In face of the European strategy for data aimed on putting people first in developing technology, and defending and promoting European values and rights in the digital world,[44] the European Commission has made digital policies a priority in its legislation, including the Data Act (DA) and the Data Governance Act (DGA).[45] The DA focuses on ensuring fair access to data generated by individuals and IoT devices, while promoting safe use of data and technologies. The DA expands on the GDPR's right to portability to non-personal data generated by connected products and related services, and its

[38] It is worth mentioning that Article 8 has experienced a slow but constant expansion of its scope. The ECHR has taken advantage of the broad formulation of such a right to adapt it to and to keep it at pace with the challenges posed by societal and technological changes. In relation to technological developments, it is worth noting the remark made by the Court in *von Hannover v. Germany* (2004). In this occasion, the Court acknowledged the need for an "increased vigilance in protecting private life" as a consequence of the evolution of communication technologies which permit to capture and store personal information about individuals on a large scale. *See von Hannover v Germany*, App.n°59320/00, (ECtHR, 24th June 2004), 70. *See also* European Court of Human Rights. Guide on Article 8 of the European Convention on Human Rights. Retrieved from https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf, 20;.

[39] Council of Europe (1981). Convention for the protection of individuals with regard to the processing of personal data (Convention 108).

[40] Kuner, C. (2012). The European Commission's proposed data protection regulation: A copernican revolution in European data protection law. *Bloomberg BNA Privacy and Security Law Report (2012) February*, *6*(2012), 1-15l; Ivanova, Y. (2021). The Role of the EU Fundamental Right to Data Protection in an Algorithmic and Big Data World. *Data Protection and Privacy: Data Protection and Artificial Intelligence*, 809, 145.

[41] Wachter, S. (2018). Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR. *Computer law & security review*, *34*(3), 436-449.

[42] Recital 3 Directive 95/46/EC Harmonisation.

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

[44] European Commision (n.d.). A European Strategy for data. Retrieve from https://digital-strategy.ec.europa.eu/en/policies/strategy-data

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

focus is on the vast amounts of data generated in the era of big data.[46] The intentions of the DA and the DGA are to preserve and complement the GDPR *acquis*.[47] Data protection law should be understood as one - albeit essential - part of a more comprehensive data law, in particular a data economy law.[48] Overall, the EU is committed to safeguarding personal data and ensuring that individuals have control over their information in the digital age. The GDPR and related legislation ensure that data protection in Europe remains at the forefront of protecting privacy in the digital world.[49]

2.1.1. The Right to the Protection of Personal Data

The right to personal data protection has become an increasingly important aspect of privacy law in Europe.[50] Over the years, in the EU data protection has evolved into a value that is not subsumed under the right to respect for private life.[51] While both have overlapping values, the EU has recognized data protection as a fundamental separate right.[52] The protection of personal data is regarded as a modern, active right, putting in place a system of control mechanisms that protect individuals every time their personal data is processed.[53] The emergence of the right to data protection is closely linked to the growing potential and the challenges presented by information and communication technology.[54] The

[46] European Commission (2022, February 23). Proposal on the Data Act. Retrieved from https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1113

[47] The European Data Protection Board & the European Data Protection Supervisor (2022, May 4). EDPB-EDPS Joint Opinion 02/2022 on the Proposal of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act). Retrieved form https://edps.europa.eu/system/files/2022-05/22-05-05_edps-edpb-jo-data-act_en.pdf. *See also* Penedo, A. C. (2022). Towards a technologically assisted consent in the upcoming new EU data laws?. *Privacy in Germany*, *5*(22), 180.

[48] The EU's legislative projects, including the Data Act, Digital Markets Act, Data Governance Act, Draft AI Regulation, Cyber Resilience Act, and GDPR, are collectively forming an economic constitution of the internal data market. *See* Lukas, L. L., & Arnold, J. F. (2023). Machine Data, Personal Data, Sensitive Data and Artificial Intelligence. the Interplay of Privacy Enhancing Technologies with the GDPR. Available at SSRN: https://ssrn.com/abstract=4341844

[49] Ivanova, Y. (2021). The Role of the EU Fundamental Right to Data Protection in an Algorithmic and Big Data World. *Data Protection and Privacy: Data Protection and Artificial Intelligence*, 809, 145.

[50] European Union Agency for Fundamental Rights (2018). Chapter 2: Data protection terminology (pp. 22). In *Handbook on European Data Protection Law*.

[51] The CJEU recognised the right to protection of personal information as a general principle in EU law as early as 1969 in the case of *Stauder* versus *the City of Ulm* (Case C-29/69). *Also see* Fuster, G. G. (2014). *The emergence of personal data protection as a fundamental right of the EU* (Vol. 16) (pp. 214). Springer Science & Business.

[52] European Union Agency for Fundamental Rights (2018). Chapter 2: Data protection terminology (pp. 22). In *Handbook on European Data Protection Law*.

[53] Advocate General Sharpston has noted that there are two separate rights in the issue at hand: the “classical” right to privacy and a more “modern” right: the right to data protection. See CJEU, Joined Cases C-92/09 and C-93/02, *Volker und Markus Schecke GbR v Land Hessen, Opinion of Advocate General Sharpston*, 17 June 2010, point 71. *See also* Mantelero, A. (2017). Regulating big data. The guidelines of the Council of Europe in the context of the European data protection framework. *Computer law & security review*, *33*(5), 584-602.

[54] Hereinafter (ICT). *See* Tzanou, M. (2021). Data Protection/Data Privacy. *Encyclopaedia entry, in Elgar Encyclopaedia of Human Rights, Forthcoming*, 6.

purpose of the GDPR is to safeguard two interests: the protection of natural persons in relation to the processing of their data and the free movement of personal data within the European Union.[55] Moreover, EU data protection law aims to strengthen individuals' fundamental rights in the digital age and facilitate business by clarifying rules for companies and public bodies in the digital single market.[56]

2.2. The Legal Definition of Personal Data: Article 4(1) GDPR

2.2.1. The Material Scope

The General Data Protection Regulation (GDPR) is a central part of the European data protection framework and is focused on the concept of personal data.[57] The qualification of data as personal is a *conditio sine qua non* for processing to be considered within the material scope of the Regulation, that is, the GDPR applies to any processing of personal data carried out with automated (wholly or in part) means.[58] Article 4(1) defines personal data as follows:

> "*any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, [...]* ".[59]

This definition is broad and includes information such as a name, identification number, location data, or online identifier that can be used to identify an individual.[60] The GDPR applies to any processing of

[55] Along with ensuring the free movement of personal data, *see* Article 1 of the GDPR.

[56] Article 1 GDPR.

[57] 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 (GDPR). 4.5.2016, OJ L 119/1, Article 4(1). *See also* Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (DPD). 24.10.1995, OJ L 281/31, Art. 2(a); Council of Europe, Convention for the protection of individuals with regard to automatic processing of personal data, ETS no. 108 of 28 January 1981 (Convention 108), Article 2(a).

[58] Dalla Corte, L. (2019). Scoping personal data: towards a nuanced interpretation of the material scope of EU data protection law. *European Journal of Law and Technology*, *10*(1).

[59] " [...] in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person", Article 4(1) provides a definition for personal data in which information is listed as an explicit substantive criterion for the existence of personal data. The Commission noted that the concept meets Parliament's wish that the definition of personal data "should be as general as possible, so as to include all information concerning an identifiable individual". *See* COM (92) 422 final, 28.10.1992, p. 10 (commentary on Article 2). *See also* WP29, Opinion 4/2007 on the Concept of Personal Data ('WP 136'), 3.

The protection of personal data is an obligation of the Data Controllers and they must organise all technological structures in an adequate system for data protection. *See also* Romansky, P. R., & S. Noninska, I. (2020). Challenges of the digital age for privacy and personal data protection. *Mathematical Biosciences and Engineering,* 17(5), 5288–5303.

[60] WP29, Opinion 4/2007 on the Concept of Personal Data ('WP 136'), 3.

personal data that is carried out with automated means, but there are two exceptions: purely personal or household activities and processing by government agencies to protect national security.[61] The GDPR requires that personal data must be processed in a lawful, fair, and transparent manner in relation to the data subject, and it must be collected for specified, explicit, and legitimate purposes only.[62] Additionally, personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.[63] The GDPR mandates stricter regulations for the processing of special categories of personal data, which are considered particularly sensitive.[64] The GDPR recognizes that these types of data pose a more significant risk to the fundamental rights of individuals and requires that they are given a higher level of protection.

2.3. The Interpretation of Personal Data Under EU-law

The definition of personal data is based in Article 4(1) of the GDPR, prescribing the elements 'any information', 'relating to', 'an identified or identifiable natural person'. However, these requirements are open to different interpretations that return a dynamic vision of it.[65] The definition of personal data is further explicated by the Article 29 Working Party (hereinafter: WP29) in Opinion 4/2007 on the concept of personal data and in the case law of the Court of Justice of the European Union (CJEU).[66] The non-binding opinions of the WP29 are an influential source for the interpretation of the concept of personal data.[67] The WP29 provided clarification on the concept by stating that the presence of four contextual elements signifies the presence of personal data (i) any information; (ii) relating to; (iii) an identified or identifiable; (iv) natural person.[68] Additionally, a three-step model has been proposed by the WP29. This model states that the processing of data must pertain to an identifiable person either

[61] Under the exemption provided for by Article 2(2), the GDPR 'does not apply to the processing of personal data […] by a natural person in the course of a purely personal or household activity' (Art. 1).

[62] Article 5(1)(a)(b) GDPR.

[63] Article 5 (1)(c)

[64] Article 9 GDPR, Processing of special categories of personal data. This includes information such as race or ethnic origin, political opinions, religious or philosophical beliefs, genetic data, biometric data, health information, and information about a person's sex life or sexual orientation.

[65] Irti, C. (2022). Personal Data, Non-personal Data, Anonymised Data, Pseudonymised Data, De-identified Data. In: Senigaglia, R., Irti, C., Bernes, A. (eds) *Privacy and Data Protection in Software Services. Services and Business Process Reengineering* (pp. 50). Springer, Singapore.

[66] Only the CJEU has authority to decide how the definition of 'personal data' should be interpreted under EU data protection law.Please be informed that as of 25 May 2018 the Article 29 Working Party ceased to exist and has been replaced by the European Data Protection Board (EDPB).

[67] The judgments of the CJEU are not nearly as comprehensive as the WP29. Most of the relevant cases simply name a particular type of data involved, ruling that this information indeed constitutes personal data. There is no discussion of what elements the concept of personal data entails and what each of those elements should mean.

[68] *See* Article 29 Working Party (2007). Opinion 4/2007 on the Concept of Personal Data ('WP 136'). Hereinafter: WP29. Hereinafter: WP29, Opinion 4/2007.

directly or indirectly in terms of content, purpose, or result.[69] The WP29 further distinguishes between provided and observed data on the one hand, and derived and inferred data, on the other.[70] Of particular interest for the present case of smart cities is the analysis of the 'relate to' (ii) and the 'identifiability' (iii) components.

2.3.1. Natural Person

Regarding the element of 'natural person' it suffices to say that only information pertaining to living natural persons rather than legal entities or deceased falls within the GDPR's scope.[71] It can therefore be concluded that data about legal entities or deceased persons do not fall within the scope of the GDPR.[72]

2.3.2. Any information

The term personal data in Article 4(1) of the GDPR is meant to be broadly applicable to any kind of information that could potentially have harmful consequences for individuals.[73] Neither the WP29 nor the CJEU have provided a clear definition of the term 'information', however it is understood to include knowledge in any form or source.[74] The lack of a specific definition can lead to confusion and misunderstandings, as the concept of personal data can encompass both factual information and subjective opinions or assessments.[75] In the *Y.S. and M.* and *S* case, it is pointed out that: "only information relating to facts about an individual can be personal data".[76] The CJEU has expanded the definition of personal data in the *Nowak case* to include all types of information, regardless of its nature, content, or format.[77] This includes information that is stored as binary code, as well as information that

[69] *See* WP29, Opinion 4/2007 on the Concept of Personal Data ('WP 136'), 10-1. Defining purpose as: "to evaluate, treat in a certain way or influence the status or behaviour of an individual".

[70] WP29 (2007). Opinion 4/2007 on the Concept of Personal Data ('WP 136'). *See also* WP29 (2016). Guidelines on the Right to Data Portability under Regulation 2016/679, WP242 rev.01,

[71] Article 2 GDPR.

[72] Article 29 Working Party (2007). Opinion 4/2007 on the Concept of Personal Data ('WP 136').

[73] Dalla Corte, L. (2020). Safeguarding Data Protection in an Open Data World: On the idea of balancing open data and data protection in the development, 234.

[74] Purtova, N. (2020). Code as personal data. *INFO-LEG* [working paper], 6.

[75] Purtova, N. (2020). Code as personal data. *INFO-LEG* [working paper], 6.

[76] *Opinion of Advocate General Sharpston in YS v Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v M and S*, Joined Cases C141/12 and C372/12, [2013], para. 56. *See also* Wachter, S., & Mittelstadt, B. (2019). A right to reasonable inferences: re-thinking data protection law in the age of big data and AI. *Colum. Bus. L. Rev., 2019*(2), 521-531.

[77]"The expression 'any information' […] reflects the aim of the EU legislature to assign a wide scope to [the concept of personal data], which is not restricted to information that is sensitive or private, but potentially encompasses all kinds of information, not only objective but also subjective, in the form of opinions and

is derived or inferred from collected data.[78] To exemplify, the WP29 interprets the notion of personal data broadly, covering all information linked to an individual, while the CJEU has yet to provide clear guidance on the meaning of information.[79] The terminology associated with personal data, encompassing both information and data as delineated in the GDPR, as well as the explications proffered by the CJEU, evinces a certain degree of ambiguity.[80]

2.3.3. Identification and Identifiability

Personal data is defined as data that can identify a natural person, either directly or indirectly.[81] Identification is an integral part of Article 4(1) of the GDPR and reflects *the raison d'être* of data protection.[82] The WP29 has made it clear that identifiability is the threshold criterion for determining whether data is considered personal.[83] The CJEU ruled for the first time on the meaning of personal data in the *Lindqvist* case. The CJEU has held that identification can occur not only through a person's name but also other means such as telephone number or information about working conditions and hobbies.[84] The WP29 has emphasised that all forms of information qualify as personal data unless the possibility of identification does not exist or is negligible.[85] If a natural person can be distinguished from others within a group, then they are considered 'identified'.[86] On the other hand, if identification has not happened yet but is possible, then the person is considered 'identifiable'.[87] The likelihood of

assessments"), Case C-434/16 *Peter Nowak v Data Protection Commissioner* (2017), ECLI:EU:C:2017:994, para 34.

[78] Case C-434/16 *Peter Nowak v Data Protection Commissioner* (2017), ECLI:EU:C:2017:994, para 33-35.

[79] It is important to note that in Nowak, the CJEU did not explicitly endorse the WP29's advice note on the meaning of 'all information' and, in general, the CJEU has yet to provide clear guidance on what the term 'information' really means. *See* Case C-434/16, *Peter Nowak v. Data Protection Commissioner* (2017), ECLI:EU:C:2017:994; WP29 (2007). Opinion 4/2007 on the Concept of Personal Data ('WP 136').

[80] *See* Case C-582/14, Patrick Breyer v. Bundesrepublik Deutschland, [2016] ECLI:EU:C:2016:779 (hereinafter Breyer); Joined Cases C-141/12 and C-372/12 YS and MS v. Minister voor Immigratie, Integratie en Asiel, (2104), ECLI:EU:C:2014:208 (hereinafter YS and others).

[81] Article 4(1) GDPR: using identifiers such as name, identification number, location data, online identifier or factors specific to an individual's physical, psychological, genetic, mental, economic, cultural or social identity. *See* Purtova, N. (2022). From knowing by name to targeting: the meaning of identification under the GDPR. *International Data Privacy Law*, *12*(3), 163-183.

[82] Purtova, N. (2022). From knowing by name to targeting: the meaning of identification under the GDPR. *International Data Privacy Law*, *12*(3), 163-183.

[83] It is important to note that opinions of the WP29 are not binding, they are authoritative.

[84] Case C-101/01 *Bodil Lindqvist,* EU:C:2003:596, para 27.

[85] It is important to note that opinions of the WP29 are not binding, they are authoritative. *See* WP29, Opinion 4/2007, 13.

[86] This is typically achieved through the above-mentioned identifiers', which signifies particular pieces of information holding a particularly privileged and close relationship with the particular individual. *See* WP29, Opinion 4/2007, 13.

[87] WP29 Opinion 4/2007, 12. *See also* Purtova, N. (2022). From knowing by name to targeting: the meaning of identification under the GDPR. *International Data Privacy Law*, *12*(3), 163-183.

identification is expressed in the 'reasonable likelihood of identification' test,[88] which takes into account all means that are reasonably likely to be used to identify the person, including the cost and time required for identification and the technology available at the time of processing.[89] The assessment should be done on a case-by-case basis and is a dynamic and context-dependent criterion, referring to the criteria of the reasonable probability of identification.[90]

In the *Breyer case* the CJEU ruled that a dynamic IP address can be considered personal data if the website publisher has the legal means to obtain additional information that enables them to identify the visitor.[91] The Court emphasised that the means of identification should be considered in light of the law and context, and that information allowing the identification of a person does not need to be in the hands of a single individual.[92] The WP29's broad interpretation of identifiability has been called into question in the context of the CJEU's decision in *Breyer*.[93] The WP29 contends that the mere possibility of distinguishing an individual is insufficient to classify them as 'identifiable', and that all relevant factors must be considered when determining the possibility of identification.[94]

In sum, information is considered personal if it relates to a person by reason of its content, purpose, or result, and the threshold condition for determining this is identifiability.[95] The WP29 has

[88] According to Recital 26 GDPR, "(...) to determine whether a natural person is identifiable, account should be taken of all the means that are reasonably likely to be used, such as detection, by the controller or another person, to identify the natural person directly or indirectly.

[89] Recital 26 of the GDPR further indicates that "the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable". The expressions of "means reasonably likely to be used" and "all objective factors" in Recital 26 substantiate the relative approach to the assessment of identifiability of a data subject. What is meant by these reasonable means does not follow directly from the GDPR. *Also see* WP29 Opinion 4/2007, 12. *See also* Purtova, N. (2022). From knowing by name to targeting: the meaning of identification under the GDPR. *International Data Privacy Law*, *12*(3), 163-183.

[90] WP29 Opinion 4/2007, 12. *See also* Finck, M., & Pallas, F. (2020). They who must not be identified—distinguishing personal from non-personal data under the GDPR. *International Data Privacy Law*, *10*(1), 11-36. *Also see* Irti, C. (2022). Personal Data, Non-personal Data, Anonymised Data, Pseudonymised Data, De-identified Data. In *Privacy and Data Protection in Software Services* (pp. 49-57). Springer, Singapore.

[91] The central issue was whether an IP address constitutes information relating to an identifiable natural person in relation to the website provider where the additional data necessary for identification of the website visitor was held by the visitor's Internet service provider. *See* para 16 of the Breyer judgement: 'it is clear from the order for the reference and the documents before the Court that internet service providers allocate to the computers of internet users either a 'static' IP address or a 'dynamic' IP address, that is to say an IP address which changes each time there is a new connection to the internet. Unlike static IP addresses, dynamic IP addresses do not enable a link to be established, through files accessible to the public, between a given computer and the physical connection to the network used by the internet service provider'. Case C-582/14, *Patrick Breyer v Bundesrepublik Deutschland* (2016) ECLI:EU:C:2016:779. *See also* De Hert, P. (2017). Data protection's future without democratic bright line rules: Co-existing with technologies in Europe after Breyer. *European Data Protection Law Review,* 3(1), 27-30.

[92] De Hert, P. (2017). Data protection's future without democratic bright line rules: Co-existing with technologies in Europe after Breyer. *European Data Protection Law Review,* 3(1), 27.

[93] Purtova, N. (2022). From knowing by name to targeting: the meaning of identification under the GDPR. *International Data Privacy Law*, *12*(3), 163-183.

[94] All relevant factors, such as the cost of identification, the intended purpose, the benefit to the controller, the interests of the data subject, as well as the risk of organisational shortcomings and technical failures, WP29 (2007). Opinion 4/2007 on the Concept of Personal Data ('WP 136'), 15.

[95] Case C-434/16, *Peter Nowak v Data Protection Commissioner* (2017), ECLI:EU:C:2017:994, 34.

indicated that the notion of identifiability is broad and that consideration must be given to technological advancements, as information that is currently unidentifiable may become identifiable in the future.[96] The core role of identification in the interpretation of personal data remains unclear, but the legally relevant chance of identification (identifiability) is the focus.[97]

2.3.4. Relating to

The element that completes the conceptualization of personal data under the GDPR is the determination of when data 'relates to' an individual. The WP29 has defined this concept as the relationship between the information and the individual.[98] This relationship is based on three elements: (i) the content of the information, (ii) the purpose of the information, (iii) and the result of the information.[99] If the information concerns a person in its content, the relationship is apparent and the data can be linked directly to the individual.[100] When the purpose of the information relates to a person, the relationship may be indirect as the data is used or is intended to be used to evaluate, treat, or influence the status or behaviour of an individual.[101] Finally, if the information relates to a person in its result, it indicates that the processing of the data is likely to impact the individual's rights and interests.[102] This impact can be sufficient even if it is not significant, and the data does not have to focus on the individual.[103]

The CJEU has given a broad interpretation to the term 'relates to', encompassing not only objective information but also subjective information.[104] According to the *Nowak* case, information will relate to an individual if it is "linked to a particular person" by reason of its content, purpose, or effect.[105] The intended and unintended impact or likelihood of impact of processing the data must also be

[96] Purtova, N. (2022). From knowing by name to targeting: the meaning of identification under the GDPR. *International Data Privacy Law,* 12(3), 163-183.

[97] WP29 (2007). Opinion 4/2007 on the Concept of Personal Data ('WP 136'), 12. *See also* Purtova, N. (2022). From knowing by name to targeting: the meaning of identification under the GDPR. *International Data Privacy Law*, *12*(3), 163-183.

[98] WP29 (2007). Opinion 4/2007 on the Concept of Personal Data ('WP 136'), 9.

[99] WP29 (2007). Opinion 4/2007 on the Concept of Personal Data ('WP 136'), 9

[100] WP29 (2007). Opinion 4/2007 on the Concept of Personal Data ('WP 136'), 10. *See also* Case C-434/16 *Peter Nowak v Data Protection Commissioner* (2017)*,* ECLI:EU:C:2017:994, para. 38-43.

[101] Finck, M., & Pallas, F. (2020). They who must not be identified—distinguishing personal from non-personal data under the GDPR. *International Data Privacy Law*, *10*(1), 11-36.

[102] Galič, M., & Gellert, R. (2021). Data protection law beyond identifiability? Atmospheric profiles, nudging and the Stratumseind Living Lab. *Computer Law & Security Review*, *40*, 105486.

[103] WP29 (2007). Opinion 4/2007 on the Concept of Personal Data ('WP 136'), 11. *See also Dalla Corte, L. (2019). Scoping personal data: towards a nuanced interpretation of the material scope of EU data protection law. European Journal of Law and Technology, 10(1).*

[104] Dalla Corte, L. (2019). Scoping personal data: towards a nuanced interpretation of the material scope of EU data protection law. *European Journal of Law and Technology*, *10*(1).

[105] Case C-434/16, *Peter Nowak v Data Protection Commissioner* (2017), ECLI:EU:C:2017:994, para. 35.

considered.[106] The determination of whether a specific data element is related to an individual is dependent on the context and can vary based on multiple factors, such as the entity in possession of the data, the purposes of processing, and the current and future technological and organisational context of processing.[107]

2.4. Anonymous and Pseudonymous data

The GDPR offers anonymization and pseudonymization as mechanisms for achieving compliance with the regulation.[108] Pseudonymization is the process of replacing identifying information of an individual with a pseudonym to decrease the linkability of the data, however, the data is still considered personal data under the GDPR.[109] Anonymization refers to the process of rendering data de-identified to the extent that it can no longer be linked to an identifiable individual, resulting in non-personal data.[110] The process of anonymization requires the data to be made irreversible in order to be considered truly anonymous.[111] However, in practice, it can be challenging to determine whether data has been adequately anonymized.[112] With the emergence of data-driven applications, the legal definition of anonymous data is now subject to uncertainty and debate.[113] This is partially because of the risk-based

[106] Case C-434/16, *Peter Nowak v Data Protection Commissioner* (2017), ECLI:EU:C:2017:994, para. 34.

[107] WP29 (2007). Opinion 4/2007 on the Concept of Personal Data ('WP 136'), 11.

[108] Esayas, S. (2015). The role of anonymisation and pseudonymisation under the EU data privacy rules: beyond the 'all or nothing' approach. *European Journal of Law and Technology*, *6*(2), 3. *See also* Dalla Corte, L. (2019). Scoping personal data: towards a nuanced interpretation of the material scope of EU data protection law. *European Journal of Law and Technology, 10(1).*

[109] 'Pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person, Article 4(5) GDPR. One simply needs to have access to the keys in order to link the data to the individual to whom they relate. Article 32(1) GDPR. *See also* Recital 26 GDPR.

[110] Dalla Corte, L. (2020). Safeguarding Data Protection in an Open Data World: On the idea of balancing open data and data protection in the development, 220.

[111] Article 29 Working Party, Opinion 05/2014 on Anonymisation Techniques (WP 216) 0829/14/EN, 6.

[112] Article 29 Working Party, Opinion 05/2014 on Anonymisation Techniques (WP 216) 0829/14/EN, 6. It should be recalled here that anonymisation is also defined in international standards such as the ISO 29100 one – being the "Process by which personally identifiable information (PII) is irreversibly altered in such a way that a PII principal can no longer be identified directly or indirectly, either by the PII controller alone or in collaboration with any other party" (ISO 29100:2011). Irreversibility of the alteration undergone by personal data to enable direct or indirect identification is the key also for ISO. From this standpoint, there is considerable convergence with the principles and concepts underlying the 95/46 Directive. This also applies to the definitions to be found in some national laws (for instance, in Italy, Germany and Slovenia), where the focus is on non-identifiability and reference is made to the "disproportionate effort" to re-identify (D, SI). However, the French Data Protection Law provides that data remains personal data even if it is extremely hard and unlikely to re-identify the data subject – that is to say, there is no provision referring to the "reasonableness" test.

[113] Finck, M., & Pallas, F. (2020). They who must not be identified—distinguishing personal from non-personal data under the GDPR. *International Data Privacy Law*, *10*(1), 11-36.

nature of anonymisation and its dependence on a variety of factors that are difficult to quantify.[114] As a result, perfect anonymization may be impossible and everything potentially becomes identified data.[115]

2.5. Non-Personal Data

The changes made to the concept of personal data have resulted in a notable enlargement of the data protection regime. Nevertheless, the framework continues to prioritise the concept of personal data as the determinant factor when assessing the applicability of the rules outlined within it. The GDPR categorises data using a binary approach,[116] whereby data is either considered personal and thus subject to the regulation or non-personal and not subject to the European data protection regime.[117] The axiom of the GDPR is that if, after exhausting all the practical means of investigation, it has been established that the information in question does not pertain to a specific or recognizable individual, or the individual is no longer recognizable, then the information must be regarded as 'non-personal' and thus exempted from the provisions of the GDPR.[118] In contrast to the restrictive regulations governing the processing of personal data, the European Union has established an additional framework for the processing of non-personal data (Regulation 2018/1807).[119] The Regulation on the free flow of non-personal data stipulates that no restrictions should be placed on the free flow of non-personal data, regardless of whether they are imposed by the public or private sector.[120] Non-personal data can thus be transferred and processed freely in the digital environment.[121] Consequently, the legal characterization of a dataset as containing personal data or not leads to the application of two regulatory

[114] Article 29 Working Party, Opinion 04/2014 on Anonymisation Techniques, 0829/14/EN; Finck, M., & Pallas, F. (2020). They who must not be identified—distinguishing personal from non-personal data under the GDPR. *International Data Privacy Law*, *10*(1), 11-36.

[115] Weitzenboeck, E. M., Lison, P., Cyndecka, M., & Langford, M. (2022). The GDPR and unstructured data: is anonymization possible?. *International Data Privacy Law*, *12*(3), 184-206.

[116] Although the proposed Data Governance Act may complicate this scenario.

[117] Recital 26 GDPR, stating that 'personal data' are "information concerning an identified or identifiable natural person", and that "to determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used (…) either by the controller or by another person to identify the natural person directly or indirectly".

[118] Finck, M., & Pallas, F. (2020). They who must not be identified—distinguishing personal from non-personal data under the GDPR. *International Data Privacy Law*, *10*(1), 14.

[119] Van der Sloot, B., Van Schendel, S., & López, C. A. F. (2022). The influence of (technical) developments on the concept of personal data in relation to the GDPR. *TILT – Tilburg Institute of Law, Technology, and Society*, 8.

[120] Van der Sloot, B., Van Schendel, S., & López, C. A. F. (2022). The influence of (technical) developments on the concept of personal data in relation to the GDPR. *TILT – Tilburg Institute of Law, Technology, and Society*, 8.

[121] Finck, M., & Pallas, F. (2020). They who must not be identified—distinguishing personal from non-personal data under the GDPR. *International Data Privacy Law*, *10*(1), 11-36.

frameworks that differ significantly.[122] It is important to note that the interpretation of non-personal data is equally important as that of personal data, as the two are dependent on each other and mutually exclusive.[123] In its comments on the framework for the free flow of non-personal data, the European Data Protection Supervisor mentioned the notion of personal and non-personal data to be 'inextricably' linked.[124] Article 3(1) of Regulation 2018/1807, asserts non-personal data as data which originally did not relate to an identified or identifiable natural person, or data which was initially personal data, but later made anonymous.[125]

As previously discussed, anonymisation can render certain information non-personal. The demarcation line between personal and non-personal data is the risk of identification: when identification is reasonably possible, the data should be considered personal.[126] While the GDPR outlines the two categories of data, in practice, a lot in between the two opposite endpoints can be considered.[127] The GDPR provides little guidance in this regard, but the Data Act and Data Governance Act can offer some insight.[128] However, substantial difficulties may arise when personal data cannot be clearly distinguished from non-personal data.[129] The dynamic and context-based nature of personal data may cause the two concepts to converge and blur, making non-personal data personal and vice versa.[130] This can occur through various techniques used, which can transform sets of data into personal data.[131]

[122] Van der Sloot, B., Van Schendel, S., & López, C. A. F. (2022). The influence of (technical) developments on the concept of personal data in relation to the GDPR. *TILT – Tilburg Institute of Law, Technology, and Society*, 8.

[123] Podda, E., & Palmirani, M. (2020). Inferring the Meaning of Non-personal, Anonymized, and Anonymous Data. In *AI Approaches to the Complexity of Legal Systems XI-XII* (pp. 269-282). Springer, Cham; Van Der Sloot, B. (2020). Regulating non-personal data in the age of Big Data. In *Health Data Privacy under the GDPR* (pp. 85-105). Routledge.

[124] Even though the EDPS argues that the concept of a mixed dataset requires further clarification. *See* EDPS, Comments of the EDPS on 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, 4. *See also* amended Recital 10: 'Where data sets contain both personal and non- personal data, Regulation (EU) 2016/679 should apply to the personal data part of the set, and this Regulation should apply to the non-personal data part of the set'.

[125] Such as data on weather conditions generated by sensors installed on wind turbines, or data on maintenance needs for industrial machines.

[126] Finck, M., & Pallas, F. (2020). They who must not be identified—distinguishing personal from non-personal data under the GDPR. *International Data Privacy Law*, *10*(1), 11-36.

[127] Finck, M., & Pallas, F. (2020). They who must not be identified—distinguishing personal from non-personal data under the GDPR. *International Data Privacy Law*, *10*(1), 11-36.

[128] The Data Act proposed regulation to establish a harmonised framework for industrial, non-personal data sharing in the European Union, mentioning IoT and smart products very explicitly in its provisions. *See* Data Act, COM/2022/68; Data Governance Act, COM/2020/767.

[129] It is debatable whether the differentiation between various categories of data remains pertinent. The underlying premise is that the handling of personal data has implications for individuals, whereas the handling of non-personal data does not.

[130] Graef, I., Gellert, R., & Husovec, M. (2018). *Towards a holistic regulatory approach for the European data economy: Why the illusive notion of non-personal data is counterproductive to data innovation*. (TILEC Discussion Paper Series; Vol. 2018, No. 29) (pp. 7).

[131] LAST-JD-RIoE (2021). Processing of home data in the light of the GDPR and IPR issues. *Law, Science and Technology Joint Doctorate: Rights of the Internet of Everything (LAST-JD-RIoE)*, 36.

Accurately determining whether data falls under the scope of the GDPR depends on properly distinguishing between personal and non-personal data.[132] The dual meaning of, on the one hand, idem, personal data, and, on the other hand, *ipse*, non-personal data, allows data to be assigned to a person.[133] Yet, non-personal data can be transformed into personal data through linkage to an identified individual.[134] Here, a low threshold to discern between personal and non-personal data is recognised.[135]

2.6. The 'Personal' in Personal Data

The term 'personal' in personal data refers to information that relates to an identifiable person.[136] The European legislator and the CJEU often use the term 'information' interchangeably with 'data'.[137] The GDPR does not specify between data and information, which adds to the complexity of defining personal data.[138] However, the increasing prevalence of emerging technologies and the various ways in which data can be extracted adds a temporal dimension to the definition of information.[139] The temporal and diachronic nature of information makes it even more challenging to distinguish between personal and non-personal data.[140] To protect personal data rights, it is crucial to establish legal certainty in

[132] Finck, M., & Pallas, F. (2020). They who must not be identified—distinguishing personal from non-personal data under the GDPR. *International Data Privacy Law*, 10(1), 11-36.

[133] Hildebrandt, M. (2015). *Smart technologies and the end (s) of law: novel entanglements of law and technology* (pp. 81). Edward Elgar Publishing.

[134] Van Der Sloot, B. (2020). Regulating non-personal data in the age of Big Data. In *Health Data Privacy under the GDPR* (pp. 85-105). Routledge.

[135] Finck, M., & Pallas, F. (2020). They who must not be identified—distinguishing personal from non-personal data under the GDPR. *International Data Privacy Law*, 10(1), 11-36.

[136] Recital 26 GDPR.

[137] In *YS and others*, AG Sharpston gives some examples of such types of data which the CJEU has explicitly pronounced personal: 'the name of a person in conjunction with his telephone coordinates or information about his working conditions or hobbies', his address, his daily work periods, rest periods and corresponding breaks and intervals,124 monies paid by certain bodies and the recipients, amounts of earned or unearned incomes and assets of natural persons. *See also* Søe, S. O., Jørgensen, R. F., & Mai, J. E. (2021). What is the 'personal' in 'personal information'?. *Ethics and Information Technology,* 23(4), 625.

[138] LAST-JD-RIoE (2021). Processing of home data in the light of the GDPR and IPR issues. *Law, Science and Technology Joint Doctorate: Rights of the Internet of Everything (LAST-JD-RIoE)*, 50.

[139] *See* WP29, Opinion 4/2007 on the Concept of Personal Data ('WP 136'), 8; ; Case C-345/17 Sergejs Buivids [2019] EU:C:2019:122, para 31. *See also* Purtova, N. (2020). Code as personal data. *INFO-LEG* [working paper], 7.; Finck, M., & Pallas, F. (2020). They who must not be identified—distinguishing personal from non-personal data under the GDPR. *International Data Privacy Law*, 10(1), 13.; Søe, S. O., Jørgensen, R. F., & Mai, J. E. (2021). What is the 'personal' in 'personal information'?. *Ethics and Information Technology,* 23(4), 625-633.

[140] Koops, B. J. (2014). The trouble with European data protection law. *International data privacy law*, *4*(4), 250-261; Gellert, R. (2021). Personal data's ever-expanding scope in smart environments and possible path(s) for regulating emerging digital technologies. *International Data Privacy Law*, 11(2), 196–208; Purtova, N. (2018). The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, *10*(1), 40-81.

determining when and to whom the GDPR applies, striking a balance between legal certainty and personal data protection as technology continues to evolve.[141]

Legal scholars have debated the broad definition of personal data and the limited exceptions to the application of data protection law, leading to the argument that all data has the potential to become personal data.[142] The advancement of technology and algorithms also creates new ways of processing data, making it more difficult to distinguish between personal and non-personal data.[143] As argued by Dalla Corte, "the concept of personal data [...] is framed diachronically: the exact same piece of information can be anonymous or personal depending on the context, actors, and time of processing".[144] The dynamic nature of data and the fluidity of what is considered personal or sensitive information means that the definition of personal data is always evolving.[145] Moreover, Purtova highlights in her work about the broad concept of personal data, the risk that the increasing datafication of society combined with the extensive scope of European data protection law might eventually make data protection 'the law of everything'.[146] The possibility of anonymization being dependent on context and state-of-the-art further complicates the distinction between personal and non-personal data.[147]

2.6.1. Does All Information Relate to Everybody?

The CJEU has interpreted the element of 'relate to' in a broad sense,[148] including information about a person (e.g. name, health status), processed with the intention of evaluating, treating or influencing the

[141] Purtova, N. (2018). The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, *10*(1), 40-81; Gellert, R. (2021). Personal data's ever-expanding scope in smart environments and possible path(s) for regulating emerging digital technologies. *International Data Privacy Law*, 11(2), 196–208.

[142] Koops, B. J. (2014). The trouble with European data protection law. *International data privacy law*, *4*(4), 250-261; Gellert, R. (2021). Personal data's ever-expanding scope in smart environments and possible path(s) for regulating emerging digital technologies. *International Data Privacy Law*, 11(2), 196–208; Purtova, N. (2018). The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, *10*(1), 40-81.

[143] Purtova, N. (2018). The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, *10*(1), 53.

[144] Dalla Corte, L. (2019). Scoping personal data: towards a nuanced interpretation of the material scope of EU data protection law. *European Journal of Law and Technology*, *10*(1), 12.

[145] Gellert, R. (2022). Comparing definitions of data and information in data protection law and machine learning: A useful way forward to meaningfully regulate algorithms?. *Regulation & Governance*, *16*(1), 156-172.

[146] Purtova, N. (2018). The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology,* 10(1), 41.

[147] Groos, D., & van Veen, E. B. (2020). Anonymised data and the rule of law. *Eur. Data Prot. L. Rev.*, *6*, 498; Weitzenboeck, E. M., Lison, P., Cyndecka, M., & Langford, M. (2022). The GDPR and unstructured data: is anonymization possible?. *International Data Privacy Law*, *12*(3), 184-206.

[148] To sum up, the CJEU generally supports the broad interpretation of identifiability in *Breyer*. The Court adopted a restrictive view on what 'information relating to' a person means in *YS and others*, suggesting that information only relates to an individual when it is about him or her. Yet in 2017 the CJEU effectively reversed

person's status or behaviour, or information that is likely to have an impact on the person's rights and interests.[149] The relation between the data subject and the information has been interpreted as based on the content, purpose, and effect of the data.[150] This interpretation of information relating to a person is gaining relevance in the age of hyper-connectivity where the same piece of data can be considered as relating to a person in one particular moment of time, and not in another, it will become increasingly difficult to distinguish between data that does and does not and will likely not impact people.[151] The regulation's technology-neutral approach manifested in the applicability to any kind of data type and processing technique, leading to covering situations where the identification of the data subject is merely potential.[152] The use of data-driven automated decision-making and data reuse can also make it challenging to assess whether data is likely to impact people.[153] The adaptable attitude of data does not seem to be considered, nor does the entire data lifecycle.[154] The relationship between the data and a person in regard to purpose and result can occur not only when the data is used but also when it is potentially or hypothetically used.[155] Considering this, the ways in which the information can be said to be relating to a natural person are manifold. By combining data, information can become personal information. For example, the fact that an unidentified person is driving a red car is not personal data, but when this fact is linked to data that can identify the person, such as the person's email address, then this fact becomes personal data.[156] In light of the definition of personal data established by the GDPR, and the interpretation as given by the WP29, any information is likely to relate to a person when used with the purpose of optimising the environment in which individuals operate and, consequently, impacting them.[157]

YS and others and its limited reading of 'relating to' in *Nowak* and extended the interpretation to include relation by reason of content, purpose or effect.

[149] Article 29 Working Party (2007), Opinion 4/2007 on the Concept of Personal Data ('WP 136'), 9–11.

[150] Volker und Markus Schecke GbR and Hartmut Eifert v. Land Hessen, joined cases no. C92/09 and C-93/09, [2010], ECR 2010 I-11063 (ECLI:EU:C:2010:662); Peter Nowak v Data Protection Commissioner, case no. C-434-16, [2017], (ECLI:EU:C:2017:994).

[151] Purtova, N. (2018). The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, *10*(1), 50.

[152] Recital 15 GDPR. *See* Dalla Corte, L. (2019). Scoping personal data: towards a nuanced interpretation of the material scope of EU data protection law. *European Journal of Law and Technology*, *10*(1)

[153] Waerdt, van de, P. (2020). Information asymmetries: recognizing the limits of the GDPR on the data-driven market. Computer Law & Security Review, 38, [105436], 12

[154] Dalla Corte, L. (2020). Safeguarding Data Protection in an Open Data World: On the idea of balancing open data and data protection in the development.

[155] See Purtova, N. (2018). The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, *10*(1), 40-8; Koops, B. J. (2014). The trouble with European data protection law. *International data privacy law*, *4*(4), 258.

[156] Solove, D. J. (2023). Data Is What Data Does: Regulating Use, Harm, and Risk Instead of Sensitive Data. *Harm, and Risk Instead of Sensitive Data* (pp. 8).

[157] Purtova, N. (2018). The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, *10*(1), 17.

2.6.2. Is Everyone Identifiable?

A natural person is identifiable when all the means reasonably likely to be used, either by the controller or by another person, to identify the data subject, directly or indirectly, are considered.[158] However, this does not render the data personal by itself: it merely makes it relatable to a person. To designate it personal, the element of identifiableness must be realised. Data becomes personal when it begins to be related to the data subject.[159] Different pieces of information, collected together, can also lead to the identification of a particular person, and constitute personal data. As priorly discussed, in the *Nowak* and *Breyer* judgments the concept of personal data is being stretched.[160] Not only objective, but also subjective information falls under the term, and it has become clear that information quickly relates to a person.[161] The key question is whether the person concerned is identifiable: how should identification under the GDPR be understood?

The WP29 affirmed in its opinion that identifiability is central to the concept of personal data and a mere possibility of associating certain information with a particular individual is enough for the data to be considered personal.[162] Hence, identifiability implies that identification has not happened yet but is possible, for example, by combining the information being processed with other information.[163] The mere possibility of associating certain information with a particular individual is sufficient. Indeed, the crux of the matter lies in determining whether the individual's identity can be reasonably determined without expending disproportionate effort.[164] One of the overarching arguments that this line of thought is based on is: "even when individuals are not 'identifiable', they may still be 'reachable'".[165]

In the *Breyer* case, the CJEU adopted an objective (or absolute) criterion, where the natural person is deemed as identifiable if any subject can do so, and rejected the subjective (or relative) criterion, for which a person is deemed identifiable if the data controller can identify a person by relying

[158] Recital 26 GDPR.

[159] Dalla Corte, L. (2020). Safeguarding Data Protection in an Open Data World: On the idea of balancing open data and data protection in the development, 235.

[160] Purtova, N. (2022). From knowing by name to targeting: the meaning of identification under the GDPR. *International Data Privacy Law*, *12*(3), 163-183.

[161] Case C-434/16 Peter Nowak (2017), EU:C:2017:582, para 34; Finck, M., & Pallas, F. (2020). They who must not be identified—distinguishing personal from non-personal data under the GDPR. *International Data Privacy Law*, 10(1), 13.

[162] The possibility of identification must be assessed given all the means reasonably likely to be used either by the controller or by another person. This possibility demands an estimate of future developments. WP29 (2007). Opinion 4/2007 on the Concept of Personal Data ('WP 136'), 12.

[163] Purtova, N. (2022). From knowing by name to targeting: the meaning of identification under the GDPR. *International Data Privacy Law*, *12*(3), 163-183.

[164] *See generally* Finck, M., & Pallas, F. (2020). They who must not be identified—distinguishing personal from non-personal data under the GDPR. *International Data Privacy Law*, *10*(1), 11-36.

[165] Barocas, S., & Nissenbaum, H. (2014). Big data's end run around anonymity and consent. *Privacy, big data, and the public good: Frameworks for engagement*, *1*, 44-75.

only on its own capacity.[166] At, *prima facie,* an extremely low threshold for considering a natural person identifiable can be extracted from this.[167]

As mentioned, to prevent creating a serious risk of circumvention, the protection of natural persons should be technologically neutral.[168] The state of technology at the time of processing must be taken into account.[169] Context here plays a crucial role. Putting the context of smart cities in place, it is important to note that the assessment of data as personal or not, nor the smart city environment itself are static, but rather dynamic and persistently developing.[170] The present criterion suggests that an individual may not be identifiable based on the data collected during the initial stage, but with the advancement of contemporary technologies, identification may become possible at a subsequent stage.[171] The aforementioned scenario may engender the prospect that all data may be deemed as personal.[172] The WP29 added in the same vein that "anonymisation is increasingly difficult to achieve with the advance of modern computer technology and the ubiquitous availability of information".[173] Subsequently, as Purtova puts it, "[t]he resulting standard of the reasonable likelihood of identification is quite broad and context-dependent, leading to one major consequence: the status of data as 'personal' is dynamic".[174] For example, (dynamic) IP addresses could not alone lead to the identification of a natural person, but possibly in combination with other data.[175] It is irrelevant whether the identification actually takes place. However, a mere hypothetical possibility of identifying someone is not sufficient to regard that person as identifiable.[176] If that possibility does not exist or is negligible, the person cannot be regarded as identifiable. As technologies to target a person are evolving, the meaning of identification

[166] *Patrick Breyer v Bundesrepublik Deutschland*, Case C-582/14, [2016] ECLI:EU:C:2016:779. 46.
[167] Dalla Corte, L. (2019). Scoping personal data: towards a nuanced interpretation of the material scope of EU data protection law. *European Journal of Law and Technology*, *10*(1).
[168] Recital 15 GDPR.
[169] Recital 15 GDPR.
[170] Gellert, R. (2021). Personal data's ever-expanding scope in smart environments and possible path(s) for regulating emerging digital technologies. *International Data Privacy Law*, 11(2), 196–208; OECD (2019). Enhancing The Contribution Of Digitalisation To The Smart Cities Of The Future. Retrieved from https://www.oecd.org/cfe/regionaldevelopment/Smart-Cities-FINAL.pdf
[171] Finck, M., & Pallas, F. (2020). They who must not be identified—distinguishing personal from non-personal data under the GDPR. *International Data Privacy Law*, *10*(1), 11-36.
[172] Purtova, N. (2018). The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, *10*(1), 40-81; Purtova, N. (2018). The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, *10*(1), 40-81.
[173] Article 29 Working Party, Opinion 03/2013 on Purpose Limitation (WP 203) 00569/13/EN, 31. *See also* Finck, M., & Pallas, F. (2020). They who must not be identified—distinguishing personal from non-personal data under the GDPR. *International Data Privacy Law*, *10*(1).
[174] Purtova, N. (2018). The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, *10*(1), 47.
[175] *Patrick Breyer v Bundesrepublik Deutschland*, Case C-582/14, [2016] ECLI:EU:C:2016:779.
[176] Purtova, N. (2018). The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, *10*(1), 40-81.

is becoming ambiguous.[177] The gap in understanding what it means to identify becomes increasingly more obvious and imperative to close.[178] The enumeration of objective factors required for identification, does not provide a definitive answer about the application. The lack of a definitive answer about the application of identifiability remains a challenge.

2.7. Conclusion

In conclusion, personal data is a critical aspect of the GDPR and is defined as information that relates to an identified or identifiable natural person. The GDPR applies to the processing of personal data carried out with automated means, except for purely personal or household activities or processing by government agencies for national security purposes. The GDPR requires that personal data must be processed in a lawful, fair, and transparent manner and must be collected for specified, explicit, and legitimate purposes only. Additionally, there are stricter regulations for the processing of special categories of personal data, which are considered particularly sensitive.

The concept of personal data under the GDPR Article 4(1) is broad and flexible to changing technology contexts.[179] It is distinguished from non-personal data, which falls outside of the scope of the GDPR.[180] However, in practice, the distinction between personal and non-personal data may not be clear, leading to legal uncertainties.[181] The low identifiability threshold and the range of ways to relate information to a person expands the material scope for EU data protection legislation, causing it to potentially regulate all computing.[182] The GDPR may be invoked not only in relation to processing personal data, but also in relation to all processed things in smart cities, leading to data protection being considered "the law of everything".[183] The boundary between personal and non-personal data has been

[177] Purtova, N. (2018). The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, *10*(1), 40-81; Earls Davis, P. A. (2020). Facial Detection and Smart Billboards: Analysing the 'Identified' Criterion of Personal Data in the GDPR. *European Data Protection Law Review*, *6*, 365.

[178] Purtova, N. (2022). From knowing by name to targeting: the meaning of identification under the GDPR. *International Data Privacy Law,* 12(3), 164.

[179] Purtova, N. (2018). The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, *10*(1), 43.

[180] Dalla Corte, L. (2019). Scoping personal data: towards a nuanced interpretation of the material scope of EU data protection law. *European Journal of Law and Technology*, *10*(1).

[181] Graef, I., Gellert, R., Purtova, N., & Husovec, M. (2018). Feedback to the Commission's Proposal on a Framework for the Free Flow of Non-Personal Data. *SSRN Electronic Journal,* 3.

[182] Purtova, N. (2020). Code as personal data. *INFO-LEG* [working paper], 1.

[183] Purtova, N. (2020). Code as personal data. *INFO-LEG* [working paper], 1.

noted to go far beyond what is immediately intuitive and the distinction between data and information may have crucial implications for ownership.[184]

[184] See Article 29 Data Protection Working Party, Opinion 04/2007 on the Concept of Personal Data 6-12 (Working Paper 136, 2013). *Also see* Quinn, P. (2021). The Difficulty of Defining Sensitive Data—The Concept of Sensitive Data in the EU Data Protection Framework. *German Law Journal, 22*(8), 1569.

Chapter III.

The Concept of Smart City

With the appearance of the Internet of Things (IoT), our living environment is getting smarter.[185] Many devices with an internet connection are therefore called 'smart'.[186] The 'smartness' refers to the devices appearing intelligent because of the large amounts of personal data they collect and analyse in real time, the capability to retrieve information from the internet, and the way they communicate with each other.[187] Smart city initiatives rely on the processing of data, often personal in nature, resulting in the applicability of the GDPR.[188] The relevance of personal data protection in 'smart' or 'datafied' cities should therefore not be overstated. To understand the impact of smart city spaces on data protection law, it is necessary to identify the technologies that are part of this hyperconnected world.

3.1. Defining Smart Cities

The concept of a smart city is an ever-evolving and holistic concept including many components.[189] There is no unequivocally accepted definition or delineation of the concept of a smart city.[190] However, it is commonly defined as a city that leverages information and communication technologies (ICT) to improve the efficiency of traditional networks and services for the benefit of its inhabitants and businesses.[191] The European Commission has defined a smart city as a place where traditional networks and services are made more efficient through the use of digital and telecommunication technologies.[192]

[185] Hereinafter: IoT. *See* Christofi, A., Wauters, E., & Valcke, P. (2021). Smart Cities, Data Protection and the Public Interest Conundrum: What Legal Basis for Smart City Processing?. *European Journal of Law and Technology*, *12*(1), 1-36.

[186] Vojković, G., & Katulić, T. (2020). Data protection and smart cities. *Handbook of smart cities*, 1-26.

[187] Van Der Sloot, B., & Lanzing, M. (2021). The continued transformation of the public sphere: on the road to smart cities, living labs and a new understanding of society. *Technology and the City: Towards a Philosophy of Urban Technologies*, 319-345.

[188] Christofi, A., Wauters, E., & Valcke, P. (2021). Smart Cities, Data Protection and the Public Interest Conundrum: What Legal Basis for Smart City Processing?. *European Journal of Law and Technology*, *12*(1), 3.

[189] Christofi, A., Wauters, E., & Valcke, P. (2021). Smart Cities, Data Protection and the Public Interest Conundrum: What Legal Basis for Smart City Processing?. *European Journal of Law and Technology*, *12*(1), 1-36.

[190] Christofi, A., Wauters, E., & Valcke, P. (2021). Smart Cities, Data Protection and the Public Interest Conundrum: What Legal Basis for Smart City Processing?. *European Journal of Law and Technology*, *12*(1), 1-36.

[191] Breuer, J., Van Zeeland, I., Pierson, J., & Heyman, R. (2019,). The Social Construction of Personal Data Protection in Smart Cities. In *2019 CTTE-FITCE: Smart Cities & Information and Communication Technology (CTTE-FITCE)* (pp. 1-6). IEEE.

[192] European Commission (n.d.). Smart cities. Retrieved from https://commission.europa.eu/eu-regional-and-urban-development/topics/cities-and-urban-development/city-initiatives/smart-cities_en

Smart cities aim to create a hyperconnected, data-driven society, relying on innovative technologies that are capable of learning and extracting knowledge from the environment.[193] All aspects of the urban environment, including the individuals living in it, are 'datafied'.[194] Smart cities collect personal data through the deployment of sensor technologies and smart devices that foster interactions with the environment. This data is then used to adapt the environment, influence individuals' behaviour, and drive economic development while enhancing the quality of life, sustainability, and accessibility.[195] The smart devices foster our interactions with the environment and both generate and collect personal data.[196] Moreover, smart cities operate on the principles of detection, recognition, prediction, and optimization.[197] They are characterised by an instrumentation and digitalization of urban areas where the interconnectedness between code and space is applied.[198] The technology behind smart cities relies on extensively processing data through sensors that communicate unobtrusively and exchange data seamlessly.[199] These sensors capture the city's surroundings and contextual attributes, allowing for a better understanding of the environment and its inhabitants.[200] For example, sensors can be used to measure air quality, noise nuisance, or track individuals across public spaces, creating vast amounts of data about them.[201]

While contributing many benefits, the development and implementation of smart cities also raises concerns about privacy and the protection of personal data. Sometimes unintentionally, sometimes with more impact than originally intended, and sometimes clashing with rights as prescribed data protection laws.[202] The exchange of information integrated into a smart city platform creates data

[193] Alaverdyan, D., Kučera, F., & Horák, M. (2018). Implementation of the smart city concept in the eu: importance of cluster initiatives and best practice cases. *International Journal of Entrepreneurial Knowledge*, *6*(1).

[194] Purtova, N. (2020). Code as personal data. *INFO-LEG* [working paper], 1-14. *Available at SSRN 3786673*

[195] Stefanouli, M., & Economou, C. (2018). Data protection in smart cities: Application of the eu gdpr. In *Conference on Sustainable Urban Mobility* (pp. 748-755). Springer, Cham.

[196] Janeček, V. (2018). Ownership of personal data in the Internet of Things. *Computer law & security review*, *34*(5), 1039-1052.

[197] Stenudd, S. (2011, May). A model for using machine learning in smart environments. In *International Conference on Grid and Pervasive Computing* (pp. 24-33). Springer, Berlin, Heidelberg.

[198] Dalla Corte, L., van Loenen, B., & Cuijpers, C. (2017). Personal Data Protection as a Nonfunctional Requirement in the Smart City's Development. In B. Anglès Juanpere, & J. Balcells Padullés (Eds.), *Proceedings of the 13th International Conference on Internet, Law & Politics: Managing Risk In the Digital Society* (pp. 29-30). Huygens Editoria.

[199] Omotubora, A., & Basu, S. (2020). Next generation privacy. *Information & Communications Technology Law*, *29*(2), 151-173.

[200] Jiang, H., Geertman, S., & Witte, P. (2022). The contextualization of smart city technologies: An international comparison. Journal of Urban Management.

[201] Stefanouli, M., & Economou, C. (2018). Data protection in smart cities: Application of the eu gdpr. In *Conference on Sustainable Urban Mobility* (pp. 748-755). Springer, Cham.

[202] Gellert, R. M. (2021). Personal data's ever-expanding scope in smart environments and possible path (s) for regulating emerging digital technologies. *International Data Privacy Law*, 11(2), 196–208

that can relate to people, and this can lead to privacy problems.[203] Service providers need to collect and process personal data to develop and run a smart city platform, and this raises immediate questions about the appropriate use and protection of this personal data.[204]

3.2. Stratumseind Living Lab

The implementation of smart cities is a gradual and ongoing process, with many cities having adopted some form of smart city technology. Nonetheless, the majority of smart city initiatives implemented thus far remain in their pilot phase and are typically funded through research and innovation grants.[205] One example of a smart city initiative is the Stratumseind Living Lab (SLL). The SLL is a smart city pilot project located in the city of Eindhoven, Netherlands.[206] This initiative is a perfect example of the concept of smart environments, which are predicated on their capability to be context-aware and adjust to the needs and desires of their users.[207] The project aims to create a sustainable and innovative urban environment through the implementation of various smart technologies and data-driven solutions with the purpose of adapting the environment and influencing individuals' behaviour.[208] The Living Lab serves as a real-life example of the concept of a smart city and how it operates, in particular with regard to personal data.[209] The main goal of the SLL is to influence behaviour and the project employs various sensors and cameras to gather data on traffic flow and pedestrian behaviour, which are then analysed to

[203] Purtova, N. (2018). The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, *10*(1), 40-81.

[204] Van Der Sloot, B. (2021). The right to be let alone by oneself: Narrative and identity in a data-driven environment. *Law, Innovation and Technology*, *13*(1), 223-255.

[205] These initiatives are subject to interpretations and may not be sustainable or repeatable in the long term. While some cities have implemented successful and scalable smart city solutions, such as smart traffic management systems or waste management solutions, these are often exceptions rather than the norm. The vast majority of smart city initiatives are still in the testing and experimentation phase, and there is a need for more sustainable and scalable solutions to be developed and implemented to fully realise the potential of smart cities. *See* Lee, J., Babcock, J., Pham, T. S., Bui, T. H., & Kang, M. (2023). Smart city as a social transition towards inclusive development through technology: a tale of four smart cities. *International Journal of Urban Sciences*, *27*(sup1), 75-100.

[206] Stratumseind is a 400 meter long nightlife street in the Netherlands with around 50 establishments such as cafes, pubs, snack bars, a nightclub and a coffee shop. Before being digitised, the street was frequently visited by young adults leading to a rise in criminal activities such as fights and vandalism. This resulted in a decline of both establishments and visitors. To change this image, the Stratumseind 2.0 project was initiated with the aim of improving the street's reputation economically and socially. *See* Van Der Sloot, B., & Lanzing, M. (2021). The continued transformation of the public sphere: on the road to smart cities, living labs and a new understanding of society. *Technology and the City: Towards a Philosophy of Urban Technologies*, 319-345.

[207] The examples given are limited real-life smart city attempts since a complete smart city doesn't exist yet.

[208] Galič, M. (2019). Surveillance, privacy and public space in the Stratumseind Living Lab: The smart city debate, beyond data. *Ars Aequi, special issue July/August*.

[209] Figueiredo, S. M., & Agyin, J. (2019). Hidden in plain sight: Toward a smart future in Eindhoven. *Architecture and Culture*, *7*(3), 493-504.

optimise the city's mobility and public safety.[210] Furthermore, the project employs data derived from smart energy meters and smart waste bins to enhance the energy efficiency and sustainability of the city.[211] The SLL highlights the potential benefits and challenges of data processing in smart cities, particularly with respect to personal data protection and privacy.[212] While data processed in Living Labs may not immediately identify individuals, it nevertheless possesses the potential to do so. As such, it is imperative to ensure that personal data is protected.[213] The thesis will employ the SLL as a case study to exemplify diverse facets of the notion of personal data and its pragmatic implementation in the context of a smart city.

3.3. Conclusion

To summarise, the smart city is an expression of a paradigm shift seeking to improve the efficiency and quality of urban living through the deployment of smart technologies.[214] It is characterised by the confluence within the built environment.[215] These technologies capture the city’s surroundings and contextual attributes, allowing for a better understanding of the environment and its inhabitants.[216] However, the development and implementation of smart cities raise concerns about privacy and the protection of personal data, which must be addressed to ensure the acceptance of successful and responsible development of smart cities.[217]

[210] Van Der Sloot, B., & Lanzing, M. (2021). The continued transformation of the public sphere: on the road to smart cities, living labs and a new understanding of society. *Technology and the City: Towards a Philosophy of Urban Technologies*, 319-345.

[211] Galič, M. (2019). Surveillance, privacy and public space in the Stratumseind Living Lab: The smart city debate, beyond data. *Ars Aequi, special issue July/August*.

[212] Van Der Sloot, B., & Lanzing, M. (2021). The continued transformation of the public sphere: on the road to smart cities, living labs and a new understanding of society. *Technology and the City: Towards a Philosophy of Urban Technologies*, 319-345.

[213] Galič, M. (2019). Surveillance, privacy and public space in the Stratumseind Living Lab: The smart city debate, beyond data. *Ars Aequi, special issue July/August*.

[214] Dalla Corte, L., van Loenen, B., & Cuijpers, C. (2017). Personal Data Protection as a Nonfunctional Requirement in the Smart City’s Development. In B. Anglès Juanpere, & J. Balcells Padullés (Eds.), *Proceedings of the 13th International Conference on Internet, Law & Politics: Managing Risk In the Digital Society* (pp. 76-92). Huygens Editoria.

[215] Boscolo, P , Bourmpos, M., Datani, I, Garre, A. G., Keunen, V., Molina-Ríos, B., Palmisano, E., & Tsiligkiri, C. (2021). Case Studies Involving the Use of Personal Data in a Smart City. In S. Topham, P. Boscolo, & M. Mulquin (Eds.)*, Personal Data-Smart Cities: How cities can Utilise their Citizen's Personal Data to Help them Become Climate Neutral* (pp. 71-95). River Publishers.

[216] Purtova, N. (2020). Code as personal data. *INFO-LEG* [working paper], 10. *See also* Van Zoonen, L. (2016). Privacy concerns in smart cities. *Government Information Quarterly*, *33*(3), 472-480.

[217] Dalla Corte, L. (2020). Safeguarding Data Protection in an Open Data World: On the idea of balancing open data and data protection in the development, 12.

Chapter IV.

Reconciling the GDPR's Definition of Personal Data with the Smart City

The increasing use of connected, data-gathering devices in public spaces raises questions about how to implement the fundamental right to data protection.[218] The interconnection of all this information, collected for the benefit of the city and its residents, affects all the data gathered, including personal data, even if the original purpose of the data processing was different.[219] The accumulation of data is likely to impact the rights and interests of individuals,[220] as the development of these cities often relies on data that may be, or can become, personally identifiable.[221] When using data in smart cities, it is important to consider how the data will be collected, stored, and used in a way that protects the privacy of citizens.[222] This leads to the legal question of how the concept of personal data can be implemented in smart cities. This chapter applies the concept of personal data, as defined in Article 4(1) of the GDPR, to the smart city environment by discussing the elements of the concept of personal data and how they apply to the data collected within a smart environment.

4.1. Personal Data in the Smart City

The WP29 has broadly defined the relationship between information and an individual to protect not only information that is already considered personal, but also information that may have the potential to become personal.[223] This broad interpretation is especially relevant in the context of smart cities, where data processing may result in information being considered personal even if the relationship

[218] Breuer, J., & Pierson, J. (2021). The right to the city and data protection for developing citizen-centric digital cities. *Information, Communication & Society*, *24*(6), 801.

[219] Gellert, R. (2021). Personal data's ever-expanding scope in smart environments and possible path(s) for regulating emerging digital technologies. *International Data Privacy Law*, 11(2), 196–208. *See also* Purtova, N. (2020). Code as personal data. *INFO-LEG* [working paper].

[220] Purtova, N. (2020). Code as personal data. *INFO-LEG* [working paper], 10. *Available at SSRN 3786673*

[221] Breuer, J., & Pierson, J. (2021). The right to the city and data protection for developing citizen-centric digital cities. *Information, Communication & Society*, *24*(6), 801.

[222] Gellert, R. (2021). Personal data's ever-expanding scope in smart environments and possible path(s) for regulating emerging digital technologies. *International Data Privacy Law*, 11(2), 196–208; Koops, B. J. (2014). The trouble with European data protection law. *International data privacy law*, *4*(4), 250-261; Purtova, N. (2020). Code as personal data. *INFO-LEG* [working paper].

[223] *See generally* WP29 (2007). Opinion 4/2007 on the Concept of Personal Data ('WP 136').

between the data and the person is not strong.[224] As the interpretation of personal data has so far left room for all types of information, the threshold for what constitutes personal data may be very low.[225]

As postulated by the GDPR, in smart cities, two types of personal data can be defined: data that can directly identify a natural person, and data that can indirectly identify a natural person.[226] The latter can be derived from secondary purposes by combining data sets.[227] Indirect personal data can pose a challenge as it is becoming easier to identify natural persons based on fragments of data and associated profiling.[228] Even software, which is a certain type of information that does not contain direct content about a person, can be classified as personal data if it falls within the WP29's broad definition of information.[229] This means that all data used, shared, and analysed in smart cities can be considered personal data, even if it does not contain direct content relating to a person, as it may have a statistical relationship with a person or lead to knowledge about a person.[230] To determine which data in the smart city environment relates to and identifies a person, the important requirements of personal data will be applied and analysed.

4.1.1. Data 'Relating to' a Person in the Smart City

When applying the element of 'relating to' a person in smart environments, there are a couple of important comments to point out. Smart environments rely on technology to process data for the purpose of adapting the environment and influencing individuals' behaviour, which often results in the processing of personal data.[231] The software used in smart cities is designed to optimise various aspects of the living environment, such as energy or water consumption, but this same software can also have the ancillary purpose of influencing individuals.[232] If information is processed with the purpose of assessing individuals or affecting their rights and interests, it is considered personal data according to GDPR's definition.[233] The software used in smart cities can be considered information that is intended

[224] "Sufficient if the individual may be treated differently from other persons as a result of the processing of such data". *See* Art. 29WP, Opinion 4/2007, p. 11.

[225] Purtova, N. (2020). Code as personal data. *INFO-LEG* [working paper], 5.

[226] No comprehensive list of personal and non-personal data connected to smart cities exists yet, and no CJEU judgement has confirmed one. *See* LAST-JD-RIoE (2021). Processing of home data in the light of the GDPR and IPR issues. *Law, Science and Technology Joint Doctorate: Rights of the Internet of Everything (LAST-JD-RIoE)*, 35.

[227] WP29 (2007). Opinion 4/2007 on the Concept of Personal Data ('WP 136').

[228] Zarsky, T. Z. (2016). Incompatible: The GDPR in the age of big data. *Seton Hall Law Review*, *47*, 995-1020.

[229] Purtova, N. (2020). Code as personal data. *INFO-LEG* [working paper], 7-9.

[230] Purtova, N. (2020). Organising concepts in law: a typology and lessons for data protection. *INFO-LEG,* 14.

[231] Art. 29WP, Opinion 4/2007; Van Zoonen, L. (2016). Privacy concerns in smart cities. *Government Information Quarterly*, *33*(3), 472-480.

[232] *See generally* Purtova, N. (2020). Code as personal data. *INFO-LEG* [working paper].

[233] Purtova, N. (2020). Code as personal data. *INFO-LEG* [working paper]; Dalla Corte, L. (2019). Scoping personal data: towards a nuanced interpretation of the material scope of EU data protection law. *European Journal of Law and Technology*, *10*(1).

to evaluate, nudge, and influence the behaviour of individuals living in these cities.[234] As this monitoring and data collection is aimed at all citizens, a significant portion of the data, by definition, will be related to an individual.[235] Therefore, it can be concluded that at least some of the data processed or the software used is related to a person either directly or indirectly, in terms of content, purpose, or result.[236]

Additionally, it is important to recognize that data is time-bound and its relationship with individuals can vary throughout its lifecycle due to its contextual nature.[237] Data in technology environments goes through different stages, such as creation, collection, processing, aggregation, storage, degradation, and potential deletion. At each stage, the data may or may not relate to a specific individual.[238] This relationship can change in an instant, and the categories of data are only temporary.[239] In the event that data is linked to a natural person based on its content, it is probable that such linkage will persist throughout the entirety of the data lifecycle, barring any alterations to the content itself.[240] Conversely, if data is linked to a natural person solely on the basis the purpose or result elements, its association with the individual will be limited to a specific period within the data lifecycle.[241]

However, if the purpose of processing is to impact the data subject from the beginning, the data can be considered personal *a priori*.[242] It is essential to distinguish between data that relates to individuals in content and data that relates in purpose or impact.[243] Even if the content does not directly relate to individuals, information can still be considered personal data if it is tied to specific individuals through auxiliary information that renders them identifiable.[244] In conclusion, data monitored, tracked,

[234] Purtova, N. (2020). Code as personal data. *INFO-LEG* [working paper], 9.

[235] Purtova, N. (2020). Code as personal data. *INFO-LEG* [working paper], 5-7.

[236] Purtova, N. (2020). Code as personal data. *INFO-LEG* [working paper], 9.

[237] Ambrose, M. L. (2012). It's about time: privacy, information life cycles, and the right to be forgotten. *Stanford Technology Law Review*, *16*, 369; Remac, M. (2017). The European Union Agency for Network and Information Security (ENISA)-Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA).

[238] Ambrose, M. L. (2012). It's about time: privacy, information life cycles, and the right to be forgotten.Stanford Technology Law Review, *16*, 369.

[239] Van Der Sloot, B. (2020). Regulating non-personal data in the age of Big Data. In *Health Data Privacy under the GDPR* (pp. 90). Routledge.

[240] Finck, M., & Pallas, F. (2020). They who must not be identified—distinguishing personal from non-personal data under the GDPR. *International Data Privacy Law*, *10*(1), 11-36.

[241] When data is considered to be related to a natural person based on its purpose or result, instead of its content, it necessitates additional auxiliary information to make the person identifiable, thereby qualifying as personal data. This implies that the information must specifically concern an identifiable data subject, rather than merely having a relation to them. *See* Dalla Corte, L. (2019). Scoping personal data: towards a nuanced interpretation of the material scope of EU data protection law. *European Journal of Law and Technology*, *10*(1), 10.

[242] Gellert, R. (2021). Personal data's ever-expanding scope in smart environments and possible path(s) for regulating emerging digital technologies. *International Data Privacy Law*, 11(2), 196–208.

[243] *See* Art 29 WP (2007). Opinion 4/2007 on the Concept of Personal Data, 11. *See also* p. 12 for the relation in impact.

[244] Auxiliary information is additional information used for identification. The relational link between the information which allows identification of a person, is justified through the purpose or the result element, rather than through content. The concept of auxiliary information is closely related to that of pseudonymised data. Indeed, it can make data subjects identified or identifiable if combined with pseudonymised data. Auxiliary

and processed in smart cities does not have to solely *focus* on someone to be considered as relating to an individual.[245] Information that relates to a data subject by virtue of its purpose or result can still be considered personal data, while information whose content relates to a data subject will remain personal data throughout its lifecycle.[246]

To illustrate the foregoing, the data collected at the SLL, the walking patterns of individuals are processed and considered as 'relating to' the individual.[247] The main goal of SLL is to gain insight into the influence of external stimuli on visitor behaviour, making all data collected at the SLL fall under the *purpose* element. Moreover, the *result* element states that information that undermines the rights and interests of an individual is considered 'relating to' the individual.[248] The WP29 stated that solely one element suffices for information to be considered 'relating to' the individual, and at least two elements apply in the case of the data processed at the SLL. Nonetheless, the definition of personal data is only useful if the individual can be proven identified or identifiable.

4.1.2. Data 'Identifying' a Person in the Smart City

The definition of personal data under the GDPR hinges on a broad definition of the notion of 'identified' or 'identifiable',[249] including auxiliary information that leads to the direct or indirect identifiability of the person.[250] As location-specific information becomes more common in smart cities, it is easier to

information leads to the identification and thus for data to be qualified as personal. Following this line of reasoning, information is considered personal data in cases where content may not directly relate to natural persons, but where it is still tied, through its purpose or result, to specific individuals through auxiliary information that renders the person identifiable. *See* Gellert, R. (2021). Personal data's ever-expanding scope in smart environments and possible path(s) for regulating emerging digital technologies. *International Data Privacy Law*, *11*(2), 196–208.

[245] *See generally* Gellert, R. (2021). Personal data's ever-expanding scope in smart environments and possible path(s) for regulating emerging digital technologies. *International Data Privacy Law*, 11(2), 196–208; Koops, B. J. (2014). The trouble with European data protection law. *International data privacy law*, *4*(4), 250-261.

[246] Dalla Corte, L. (2020). Safeguarding Data Protection in an Open Data World: On the idea of balancing open data and data protection in the development, 233.

[247] Galič, M. (2019). *Surveillance and privacy in smart cities and living labs: Conceptualising privacy for public space* (pp. 56) [PhD-Thesis – Research and graduation external, Tilburg University]. Optima Grafische Communicatie.

[248] Galič, M. (2019). *Surveillance and privacy in smart cities and living labs: Conceptualising privacy for public space* (pp. 56) [PhD-Thesis – Research and graduation external, Tilburg University]. Optima Grafische Communicatie.

[249] Article 4(7) GDPR and Recital 26 GDPR The determination of whether data is personal or not is a dynamic process that takes into account the means available to both the data controller and any third party.

[250] Such as unique identifiers like cookies, *see* Article 29 Working Party opinion 4/2007 on the concept of personal data, 20 June 2007, 12. *See also* Article 29 Working Party (2011), Opinion 16/2011 on EASA/IAB Best Practice Recommendation on Online Behavioural Advertising (WP 188), 8. *See also* Article 29 Working Party opinion 4/2007 on the concept of personal data, 20 June 2007, 13-14.; Borgesius, F. J. Z. (2016). Singling out people without knowing their names–Behavioural targeting, pseudonymous data, and the new Data Protection Regulation. *Computer Law & Security Review*, *32*(2), 256-271.

relate data to identifiable individuals, including metadata and geodata.[251] In essence, this information is 'information about information',[252] and can contain personal information, even if the purpose is to improve mobility and safety.[253] A noteworthy point is that in smart environments, all individuals can be deemed 'identifiable' on the basis that identification has not yet occurred, but remains a possibility.[254] All forms of information can qualify as personal data unless the possibility of identification does not exist or is negligible.[255] With the increasing number of situations in which identification is inherent in smart cities, the concept of identifiable persons will soon extend to cover everything in the environment.[256]

Taking the example of the SLL, the information collected, such as temperature, sunshine hours, rain volume, and wind speed,, is considered personal data as it is collected in a database and can be used to assess and influence behaviour.[257] The information may not pertain to a specific individual, but it still relates to the individual in purpose and impact.[258] When combined with other data sources, such as WiFi tracking sensors, voice recordings, and video footage, the data from the weather station can easily lead to the identification of an individual. Thus, the weather information is considered personal data falling within the scope of the GDPR.[259] Subsequently, even if the SLL takes steps to anonymize or pseudonymize the information, the collection of various other types of data that can be combined to infer and identify individuals means that the information remains 'related to an identifiable individual' as per Recital 26(2) of the GDPR.[260] The SLL illustrates how seemingly neutral information such as that related to weather can be considered personal data under Article 4(1) GDPR.[261]

[251] In this situation, metadata does not include the content of the conversation, but the telephone number you call, how long you call and which telephone masts you are connected to. *See* Purtova, N. (2018). The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, *10*(1), 40-81.

[252] Finck, M., & Pallas, F. (2020). They who must not be identified—distinguishing personal from non-personal data under the GDPR. *International Data Privacy Law, 10*(1), 11-36.

[253] Purtova, N. (2018). The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, *10*(1), 40-81.

[254] WP29 Opinion 4/2007, 12. *See also* Purtova, N. (2022). From knowing by name to targeting: the meaning of identification under the GDPR. *International Data Privacy Law*, *12*(3), 163-183.

[255] WP29, Opinion 4/2007, 13.

[256] Coetzee, S., Ivánová, I., Mitasova, H., & Brovelli, M. A. (2020). Open geospatial software and data: A review of the current state and a perspective into the future. *ISPRS International Journal of Geo-Information*, *9*(2), 90.

[257] Purtova, N. (2018). The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, *10*(1), 58.

[258] WP29 (2007). Opinion 4/2007 on the Concept of Personal Data ('WP 136'), 9.

[259] Coetzee, S., Ivánová, I., Mitasova, H., & Brovelli, M. A. (2020). Open geospatial software and data: A review of the current state and a perspective into the future. *ISPRS International Journal of Geo-Information*, *9*(2), 90.

[260] El Khoury, A. (2018). Personal Data, Algorithms and Profiling in the EU: Overcoming the Binary Notion of Personal Data through Quantum Mechanics. *Erasmus Law Review*, *11*, 172.

[261] Purtova, N. (2018). The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, *10*(1), 58.

4.2. Conclusion

The development of smart cities promises to bring convenience to our lives through the use of technology. However, this convenience comes at the cost of collecting vast amounts of personal data, leading to legal uncertainty. The GDPR is designed to protect people against the unauthorised collection or use of their personal data in public spaces. However, the nature of smart cities and the associated technologies conflicts with the concept of personal data, which is focused on regulating clearly distinguishable information types.[262] In a hyperconnected world, all information can relate to a person in some way, which means that the notion of personal data extends in smart technology settings.[263] The data produced and collected through smart applications can be tied to individuals, making the concept of personal data strictly context, time, and technology dependent.[264] Any information can fall under the concept of personal data, which creates uncertainty around which datasets are not personal data.[265] Moreover, even the ease with which an individual can be identified in anonymous datasets adds to this uncertainty.[266]

The example of the SLL demonstrates that the types of data collected and processed at the living lab can be considered personal data if they can be related to an identifiable natural person, regardless of whether it was collected in a private or public setting. Therefore, smart cities are not exempt from data protection obligations because they are considered public places. The collection of various types of data that can be combined to infer and identify individuals means that the information remains ‘related to an identifiable individual’ as per the GDPR. It is foreseeable that individuals will be identified through the data, as technology companies and other actors have the means, such as re-identification techniques, to uncover previously unknown information from large databases.[267]

It is appropriate for individuals to exercise control over their personal data within smart cities, but it would be up to the courts to decide whether individuals are indeed warranted protection under the GDPR. There is an inherent tension between the concept of personal data and the application of smart

[262] Unless those means are practically impossible or illegal. *See* CJEU, Patrick Breyer v Bundesrepublik Deutschland (n 845), 46.

[263] Purtova, N. (2020). Code as personal data. *INFO-LEG* [working paper], 5.

[264] Dalla Corte, L. (2020). Safeguarding Data Protection in an Open Data World: On the idea of balancing open data and data protection in the development, 235.

[265] Purtova, N. (2018). The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, *10*(1), 40-81.

[266] Veale, M., Binns, R., & Edwards, L. (2018). Algorithms that remember: model inversion attacks and data protection law. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, *376*(2133), 8.

[267] Galič, M. (2019). *Surveillance and privacy in smart cities and living labs: Conceptualising privacy for public space* [PhD-Thesis – Research and graduation external, Tilburg University]. Optima Grafische Communicatie.

technologies. It will be crucial to determine the appropriate balance between personal data protection, on the one hand, and innovation and convenience in the smart city. In conclusion, the concept of personal data needs to be considered carefully when developing smart cities to protect individual privacy and ensure that these technological advancements benefit society as a whole.[268]

[268] Hildebrandt, M. (2016). Law as Information in the Era of Data Driven Agency. *The Modern Law Review*, *79*(1), 1-30; Van Zoonen, L. (2016). Privacy concerns in smart cities. *Government Information Quarterly*, *33*(3), 472-480.

Chapter V.

The Paradox of Personal Data in the Smart City

The rise of smart cities is accompanied by a growing threat to personal data.[269] The digital connectivity of smart cities leads to the collection and exposure of vast amounts of data, which may fall under the scope of the GDPR.[270] The context of the data is key to its definition as personal data, and without proper contextualization, the personal data is becoming a non-functional requirement.[271] Technological developments have an effect on how current data protection legislation is structured.[272] As such, the smart city concept presents challenges to traditional data protection practices and raises questions about the definition of personal data.[273] In light of the aforementioned challenges, inquiries have arisen regarding just how the legal regime should respond. One such inquiry pertains to the potential expansion of the definition of personal data to encompass almost any type of data. However, it is worth considering whether such expansion would lead to the treatment of all data as personal data in practice.[274] This chapter will examine the potential challenges that the concept of personal data faces in smart cities.

5.1. The All-Encompassing Scope of Personal Data in the Smart City: A Meaningless Concept?

The scope of personal data under the GDPR has become so extensive that it is anticipated that almost all things information will eventually fall under its purview, necessitating the application of data

[269] Purtova, N. (2018). The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, *10*(1), 43.
[270] Denker, A. (2021). Protection of Privacy and Personal Data in the Big Data Environment of Smart Cities.The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences, XLVI-4/W5-2021, 181-186.
[271] Talebkhah, M., Sali, A., Marjani, M., Gordan, M., Hashim, S. J., & Rokhani, F. Z. (2021). IoT and big data applications in smart cities: recent advances, challenges, and critical issues. *IEEE Access*, *9*, 55465-55484.
[272] Van der Sloot, B., Van Schendel, S., & López, C. A. F. (2022). The influence of (technical) developments on the concept of personal data in relation to the GDPR. *TILT – Tilburg Institute of Law, Technology, and Society*, 8.
[273] Brown, T. E. (2019). Human Rights in the Smart City: Regulating Emerging Technologies in City Places. *Regulating New Technologies in Uncertain Times*, 47-65.
[274] Van der Sloot, B., Van Schendel, S., & López, C. A. F. (2022). The influence of (technical) developments on the concept of personal data in relation to the GDPR. *TILT – Tilburg Institute of Law, Technology, and Society*, 65-213.

protection to all aspects of life.[275] Pursuant to Article 4(1) GDPR, any information that can be linked to an individual is considered personal data, creating complications in smart cities, where all information is interlinked.[276] Any data associated with personal data automatically becomes personal data, even if it cannot be linked to a particular individual in isolation.[277] In a smart environment, the comprehensive definition of personal data, coupled with the narrow exemptions under data protection law, has resulted in the processing of all data as personal data, including but not limited to information obtained from traffic cameras, road sensors, energy consumption, connected vehicles, and many other sources.[278] This is illustrated by the inferred data from recorded eye activities, which may reveal sensitive information about an individual.[279] Despite its primary purpose of enhancing road safety, this technology can potentially lead to the disclosure of personal data that is more intrusive to individuals than the data itself.[280] The application of inferential analytics to collected data is considered personal data in the manner envisaged by Article 4(1) GDPR, adding to the growing scope of personal data in smart cities.[281]

[275] *See generally* Purtova, N. (2018). The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, *10*(1), 40-81.

[276] Purtova, N. (2018). The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, *10*(1), 40-81.

[277] Solove, D. J. (2023). Data Is What Data Does: Regulating Use, Harm, and Risk Instead of Sensitive Data. *Harm, and Risk Instead of Sensitive Data* (pp. 7).

[278] Christofi, A. (2021). Smart cities and the data protection framework in context. *SPECTRE,* 8.

[279] Eye activity recording is a technology used for driver safety in which cameras are used to monitor the driver's eye movements to detect drowsiness or distraction. For example, if the camera captures the driver wearing glasses, the inference can be made that the driver may have a vision impairment. Similarly, if the camera captures the driver looking at a specific location, it can be inferred that the driver is potentially interested in or affected by what is happening in that location. The following categories of personal information can be inferred from eye-tracking data: voice recordings, accelerometer data, and video game data. Therefore, the mere recording of eye activities for driver safety can have privacy implications and needs to be evaluated carefully to ensure that individuals' privacy rights are protected. *See* Kröger, J. L. (2022). *Rogue Apps, Hidden Web Tracking and Ubiquitous Sensors* [Doctoral dissertation, Universität Berlin], 222–225; Kröger, J. L., Lutz, O. H. M., Müller, F. (2020). What Does Your Gaze Reveal About You? On the Privacy Implications of Eye Tracking. In Friedewald, M., Önen, M., Lievens, E., Krenn, S., Fricker, S. (Eds.), *Privacy and Identity Management. Data for Better Living: AI and Privacy. Privacy and Identity*. IFIP Advances in Information and Communication Technology (Vol. 576. pp. 226–241).

[280] The drawing of inferences from collected personal data is increasingly seen as a threat to individual privacy, more so than the mere collection and storage of the data itself. However, the concept of personal data as defined in the GDPR is not exhaustive and it is not entirely clear whether inferences drawn from personal data fall under this definition, particularly given the effectiveness of AI in this area. This ambiguity has been criticised as a legal loophole, with experts calling for greater clarity and regulation of inferred data. While some inferences can be verified, others are subjective and cannot be confirmed, at least not at present. Nevertheless, any information or assessment about a person, whether verified or unverifiable, can have real consequences for the individual. As inference methods become more accurate and efficient with technological advances, the potential impact on people's lives increases. Therefore, it is argued that inferences about individuals should be subject to data protection law, regardless of their verifiability, as they may still have a significant impact on individuals. However, whether this really is mandated by the law ultimately depends on a case-by case assessment. *See* Kröger, J. L. (2022). *Rogue Apps, Hidden Web Tracking and Ubiquitous Sensors* [Doctoral dissertation, Universität Berlin], 222–225.

[281] Inferences can fulfil all four elements required for data to constitute personal data under Art. 4(1) GDPR, which is partly due to the broad scope of the CJEU, and the Art. 29 WP ascribe to the definition. *See* Fischer, C.

Currently, data as a source of information leads to a paradoxical situation where all data can potentially become personal data.[282] The multifaceted nature of the concept has led to an impractical approach to data protection law.[283] The differentiation between personal and non-personal data has become progressively volatile and fluid, rendering it open to interpretation.[284] The integration of smart technology in urban environments makes it highly likely that non-personal data can become personal data, and even anonymous data can be re-identified.[285] The GDPR does not address the issue of mixed data, nor does it provide guidance on how to distinguish personal data within a single data set.[286] However, it is crucial to recognize and tackle this matter rather than neglecting it.[287]

Furthermore, the GDPR's broad and inclusive objectives can make it challenging to determine the boundaries of personal data.[288] Some legal scholars argue that an overly expansive interpretation of personal data protection can hinder innovation and economic development,[289] while still leading to widespread profiling and surveillance that could have a chilling effect on individual freedom and democratic accountability.[290] The dynamic nature of data and the pervasiveness of technology in smart

(2020). The legal protection against inferences drawn by AI under the GDPR [L.L.M. thesis]. *Tilburg Law School, LL.M. Law and Technology*, 40. With regard to the risk of spurious correlations and incorrect inferences, the Article 29 Working Party has pointed out that it is "crucial that data subjects/consumers are able to correct or update" data inferred about them. *See* Article 29 Working Party (2013). Opinion 03/2013 on purpose limitation. Tech. rep. 00569/13/EN WP 203. Retrieved from https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en. pdf.

[282] Janeček, V. (2018). Ownership of personal data in the Internet of Things. *Computer law & security review*, *34*(5), 1043.

[283] Koops, B. J. (2014). The trouble with European data protection law. *International data privacy law*, *4*(4), 250-261. *See also* Van Der Sloot, B. (2020). Regulating non-personal data in the age of Big Data. In *Health Data Privacy under the GDPR* (pp. 85-105). Routledge.

[284] Van der Sloot, B., & van Schendel, S. (2021). Procedural law for the data-driven society. *Information & Communications Technology Law*, *30*(3), 311.

[285] For example, a dataset that contains personal data may be linked and enriched with another dataset and become a set that contains sensitive data. Then the data may then be aggregated or stripped from their identifiers and become non-personal data. Subsequently, the data may be de-anonymised or integrated in another dataset containing personal data again. The subsequent steps may happen in a split second. Data is therefore highly volatile and fluid. As a consequence, it is becoming increasingly difficult to determine whether the data used is personal or not and thus whether to comply with the GDPR. The question is not only what falls under the definition of 'personal data', 'metadata', 'anonymous data' or 'sensitive personal data'. *See* Koops, B. J. (2014). The trouble with European data protection law. *International data privacy law*, *4*(4), 250-261. *See also* Tzanou, M. (2020). The GDPR and (big) health data: Assessing the EU legislator's choices. In *Health Data Privacy under the GDPR* (pp. 3-22). Routledge.

[286] Vardanyan, L., & Kocharyan, H. The GDPR and the DGA Proposal: are They in Controversial Relationship?. *European Studies*, *9*(1), 91-109.

[287] Ufert, F. (2020). AI regulation through the lens of fundamental rights: How well does the GDPR address the challenges posed by AI?. *European Papers-A Journal on Law and Integration*, *2020*(2), 1087-1097.

[288] Daoudagh, S., Marchetti, E., Savarino, V., Bernabe, J. B., García-Rodríguez, J., Moreno, R. T., ... & Skarmeta, A. F. (2021). Data Protection by Design in the Context of Smart Cities: A Consent and Access Control Proposal. *Sensors*, *21*(21), 7154.

[289] Ohm, P. (2009). Broken promises of privacy: Responding to the surprising failure of anonymization. *UCL Law Review*, *57*, 1701.

[290] Korff, D., & Shadbolt, N. (2010). Public information: Cause for celebration or concern?. *Public and Science*, 10-11.

cities is expanding to include all information, regardless of its ability to identify the data subject on its own.[291] The smart city revolves primarily around data, and any element has the potential to serve as a source of data.[292] This approach does not recognize that situations involving personal data are not all the same and should not be protected in the same way.[293] The concept of personal data is becoming blended, arbitrary, and incoherent, leading to a situation where data categories are so interwoven that it is impossible to separate them.[294] The current regime distinguishing categories of personal data is losing its relevance.[295] The over-extension of the concept of personal data leads to a situation in which the concept becomes meaningless.[296] This results in a situation where the concept covers everything and yet means nothing.[297] The growth and accessibility of personal data in smart cities is contributing to the erosion of its definition and rendering it futile.

5.2. System Overload: The Blurred Lines of Personal Data in a Connected World.

It has become apparent that the concept of personal data holds the potential to be all-encompassing,[298] yet there are no clear answers about what data qualifies as personal data in the current smart city scenario.[299] Smart cities have transformed the traditional approach where individuals themselves provide personal data,[300] generating vast amounts of new types of data through devices, sensors, and

[291] Gellert, R. (2021). Personal data's ever-expanding scope in smart environments and possible path(s) for regulating emerging digital technologies. *International Data Privacy Law*, 11(2), 196–208.

[292] Omotubora, A., & Basu, S. (2020). Next generation privacy. *Information & Communications Technology Law*, *29*(2), 155.

[293] Solove, D. J. (2023). Data Is What Data Does: Regulating Use, Harm, and Risk Instead of Sensitive Data. *Harm, and Risk Instead of Sensitive Data* (pp. 43).

[294] Solove, D. J. (2023). Data Is What Data Does: Regulating Use, Harm, and Risk Instead of Sensitive Data. *Harm, and Risk Instead of Sensitive* Data (pp. 43).

[295] Rhoen, M. H. C. (2019). *Big data, big risks, big power shifts: Evaluating the General Data Protection Regulation as an instrument of risk control and power redistribution in the context of big data*. [PhD-Thesis – Research and graduation external, Leiden University].

[296] Solove, D. J. (2023). Data Is What Data Does: Regulating Use, Harm, and Risk Instead of Sensitive Data. *Harm, and Risk Instead of Sensitive Data* (pp. 1-50).

[297] As Purtuva pointed on, ‘playing devil’s advocate’, even weather is personal data in a smart environment. *See* Purtova, N. (2018). The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, *10*(1), 57.

[298] Purtova, N. (2018). The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, *10*(1), 43.

[299] Solove, D. J. (2023). Data Is What Data Does: Regulating Use, Harm, and Risk Instead of Sensitive Data. *Harm, and Risk Instead of Sensitive Data* (pp. 8).

[300] Gellert, R. (2021). Personal data's ever-expanding scope in smart environments and possible path(s) for regulating emerging digital technologies. *International Data Privacy Law*, 11(2), 196–208.

networks, including inferred, derived, and aggregate data.[301] The GDPR's arbitrary classifications and blurred lines make it challenging to apply a level of protection to a dataset at a specific moment in time,[302] as the status of data is constantly changing.[303] The speed of data creation, collection and sharing also renders information quickly obsolete, making it challenging to determine the status of a datapoint at any given moment.[304] This sheds light on the open-ended, unstable and ambulatory side of the concept.[305]

The constantly evolving nature of technology and its impact on the value of data create tension with the static conceptualization of data under the GDPR.[306] What once was considered personal information may not be considered so in another place or time, and this momentary character of technology challenges the notion of personal data.[307] This complexity demands careful consideration and continuous adaptation to changing technological realities, as compliance with the Regulation in practice becomes more difficult.

5.2.1. The Synergism of the Elements

Despite the GDPR's aim to strike a balance, the requirement of data 'relating to' and 'an identified or identifiable' natural person as currently interpreted and applied is impractical in a smart city.[308] Smart technology blurs the line between personal and non-personal data, challenging the concept of personal data and its relationship with non-personal data.[309] With the possibility of multiple data profiles and re-identification of data, personal and non-personal data are becoming harder to distinguish.[310] Technology

[301] Solove, D. J. (2023). Data Is What Data Does: Regulating Use, Harm, and Risk Instead of Sensitive Data. *Harm, and Risk Instead of Sensitive Data* (pp. 1-50).

[302] Dalla Corte, L., van Loenen, B., & Cuijpers, C. (2017). Personal Data Protection as a Nonfunctional Requirement in the Smart City's Development. In B. Anglès Juanpere, & J. Balcells Padullés (Eds.), Proceedings of the 13th International Conference on Internet, Law & Politics: Managing Risk In the Digital Society (pp. 76-92). Huygens Editorial.

[303] Heidegger, M. (1977) The Question Concerning Technology, in: *The Question Concerning Technology and Other Essays*,W. Lovitt (trans.) (New York, Harper and Row), pp. 3– 35.

[304] Omotubora, A., & Basu, S. (2020). Next generation privacy. *Information & Communications Technology Law*, *29*(2), 151-173.

[305] Van Der Sloot, B. (2020). Regulating non-personal data in the age of Big Data. In *Health Data Privacy under the GDPR* (pp. 94). Routledge.

[306] Crețu, A. M., Monti, F., Marrone, S., Dong, X., Bronstein, M., & de Montjoye, Y. A. (2022). Interaction data are identifiable even across long periods of time. *Nature communications*, *13*(1), 1-11.

[307] Heidegger, M. (1977) The Question Concerning Technology, in: *The Question Concerning Technology and Other Essays*,W. Lovitt (trans.) (New York, Harper and Row), pp. 3– 35.

[308] Purtova, N. (2018). The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, *10*(1), 56.

[309] Tene, O., & Polonetsky, J. (2012). Big data for all: Privacy and user control in the age of analytics. *Northwestern Journal of Technology and Intellectual Property*, *11*, 258.

[310] Purtova, N. (2018). The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, *10*(1), 56.

gradually erodes what formerly was characterised as personal data.[311] The semantics of data, being either personal or non-personal, are changing in smart environments, where technology erodes what was once considered personal data. The law cannot protect information solely based on whether it is expected to be personal or not.[312] The exchange of identifiers is a necessary component of technology, making identifiability and relation to an individual almost inherent in smart environments.[313] Opaque, complex data flows and ubiquitous capture of data that can 'link' a piece of information to a person can constitute personal data as referred to in the GDPR.[314] Even regular video surveillance systems or smart-home devices can be considered personal data if linked to a name or address.[315]

At the other end of the spectrum, even when an individual is not identified based on existing data, they may still be reachable and personal data may still be processed.[316] For example, in the case of automatic processing of personal data, the Council of Europe has argued that even if based on an anonymous profile, the application of the profile to individuals entails that these individuals are *at least* identifiable, signifying that personal data is processed since the moment of collection.[317] The problem with the concept of personal data based on information 'relating to' and 'identifying' a person is that it ensnares the law into a debate over the meaning of personal data and takes the focus away from the full range of problems the law needs to address.[318] For example, when personal data is anonymized, it is no longer identifiable and is therefore no longer considered personal data. However, if the anonymized data can be re-identified by combining it with other data sources, it can become personal data again. If the information in question is related to the data subject based on its content, the information itself may have personal significance and thus make the data subject identifiable.[319] On the other hand, when the link between the information and the data subject is based on the purpose or result, additional

[311] Solove, D. J. (2010). Fourth amendment pragmatism. *Boston College Law Review*, *51*, 1524.

[312] Finck, M., & Pallas, F. (2020). They who must not be identified—distinguishing personal from non-personal data under the GDPR. *International Data Privacy Law*, *10*(1), 11-36.

[313] De Conca, S. (2021). *The enchanted house: An analysis of the interaction of intelligent personal home assistants (IPHAs) with the private sphere and its legal protection* (pp. 145).

[314] Purtova, N. (2018). The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, *10*(1), 40-81.

[315] Ohm, P., & Peppet, S. (2016). What If Everything Reveals Everything?. *Big Data Is Not a Monolith (MIT Press 2016)*.

[316] As stressed in *Breyer* "(i)t would never be possible to rule out, with absolute certainty, the possibility that there is no third party in possession of additional data which may be combined with that information and are, therefore, capable of revealing a person's identity". *See* Opinion of AG Campos Sànchez-Bordona in case *Breyer v Germany*, C-582/14, 12 May 2016, ECLI:EU:C:2016:339, 67-68. *See also* Barocas, S., & Nissenbaum, H. (2014). Big data's end run around anonymity and consent. *Privacy, big data, and the public good: Frameworks for engagement*, *1*, 44-75.

[317] Council of Europe (2010), The Protection of Individuals with Regard to Automatic Processing of Personal Data in the Context with Regard to Automatic Processing. *Recommendation CM/Rec(2010)13 and Explanatory Memorandum*, para 57.

[318] Solove, D. J. (2010). Fourth amendment pragmatism. *Boston College Law Review*, *51*, 1511-1538.

[319] Dalla Corte, L. (2019). Scoping personal data: towards a nuanced interpretation of the material scope of EU data protection law. *European Journal of Law and Technology*, *10*(1), 10.

information is needed to satisfy the identifiability requirement and classify the data as personal.[320] In essence, the classification of data as pertaining to a natural person through the purpose or result element inherently sets a higher bar for achieving identifiability, in contrast to when the information pertains to the data subject based on its content.[321] This interplay between the concepts of 'identifiability' and 'relating to' generates a level of ambiguity in the definition of personal data.[322] Thus, the definition of personal data is a multifaceted matter that is further complicated by the interaction of these two fundamental components.[323]

Without a thorough understanding of what it means to identify somebody, any debate surrounding identifiability is at risk of being meaningless. As technology continues to advance and pushes the limits of data protection, the meaning of identification becomes increasingly vague.[324] The fundamental absence of a progressive understanding of data in light of modern technology highlights the need to bridge the gap in our understanding of this concept.[325] The GDPR should adopt a more pragmatic approach to the concept of personal data and the EU should directly face the issue of how to regulate personal information gathering in smart cities.[326] The ongoing discussions regarding the boundaries of data protection law are significant. However, the law should not be directed only at the protection of certain information based on whether it is expected to be personal or not. Instead of engaging in a fruitless exercise of determining whether or not personal data is processed, the law should focus on addressing a broad range of problems and safeguarding practical solutions.[327]

[320] In this case, the data only becomes personal when combined with auxiliary data that can lead to the identification of the related natural person. If the data alone can lead to the identification of the data subject, the relational link is based on content, without the need to rely on purpose or result elements, *see* Dalla Corte, L. (2019). Scoping personal data: towards a nuanced interpretation of the material scope of EU data protection law. *European Journal of Law and Technology*, *10*(1), 10.

[321] Dalla Corte, L. (2019). Scoping personal data: towards a nuanced interpretation of the material scope of EU data protection law. *European Journal of Law and Technology*, *10*(1), 10.

[322] Purtova, N. (2022). From knowing by name to targeting: the meaning of identification under the GDPR. *International Data Privacy Law*, *12*(3), 164.

[323] Purtova, N. (2022). From knowing by name to targeting: the meaning of identification under the GDPR. *International Data Privacy Law*, *12*(3), 164.

[324] Purtova, N. (2022). From knowing by name to targeting: the meaning of identification under the GDPR. *International Data Privacy Law*, *12*(3), 164.

[325] Van der Sloot, B., & van Schendel, S. (2021). Procedural law for the data-driven society. *Information & Communications Technology Law*, *30*(3), 304-332.

[326] Solove, D. J. (2010). Fourth amendment pragmatism. *Boston College Law Review*, *51*, 1511-1538.

[327] Ohm, P., & Peppet, S. (2016). What If Everything Reveals Everything?. *Big Data Is Not a Monolith (MIT Press 2016).*. *See also* Purtova, N. (2018). The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology, 10*(1), 40-8.; Van Loenen, B., Kulk, S., & Ploeger, H. (2016). Data protection legislation: A very hungry caterpillar: The case of mapping data in the European Union. *Government Information Quarterly*, *33*(2), 338-345.

5.2.2. Distinguishing Information from Data: Avoiding Conflation

The concept of personal data is rooted in the broad definition of information and the legal definition of personal data is based on the semantic understanding of 'information'.[328] This concept is limited because it focuses on the information relating to an identified person, whereas (smart) technologies are about knowledge and the inference and creation thereof.[329] The relationship between information and a person is the source of problems.[330] The insufficient regulation of inferred information has been recognized as a significant loophole of the GDPR.[331] The changing nature of personal data has highlighted the challenge of the existing understanding of the value of these concepts and interaction between individuals, technology, and the environment.[332] The influence of technology shines a spotlight on the unstable semantics of the GDPR under the spotlight.[333]

Data and information are distinct concepts with differing legal implications for personal data.[334] Although significant, the line between data and information can be difficult to discern in practice, resulting in a degree of indeterminacy in the definition of personal data established by the GDPR.[335] In light of the ambiguity in the concept of data and its implications for the protection of personal data, it is imperative to undertake a meticulous analysis and interpretation of data to ascertain whether it falls within the definition of personal data as provided by the GDPR.[336] The GDPR refers to 'information'

[328] Ducuing, C. (2021). The regulation of 'data': a new trend in the legislation of the European Union? *KU Leuven*

[329] Hildebrandt, M. (2006). Profiling: From data to knowledge: The challenges of a crucial technology. *Datenschutz und Datensicherheit-DuD*, *30*(9), 550. *See also* Gellert, R. M. (2021). Personal data's ever-expanding scope in smart environments and possible path (s) for regulating emerging digital technologies. *International Data Privacy Law*, 11(2), 208.

[330] This is because the WP29 interpretation of the definition of personal data includes "any information" that meets the other criteria of the definition, regardless of content or format: " [...] content, format, medium, or form, which could be 'alphabetical, numerical, graphical, photographical or acoustic', 'kept on paper [or] stored in a computer memory' as a binary code, structured or unstructured", WP29 (2007). Opinion 4/2007 on the Concept of Personal Data ('WP 136'), 6–9. *See also* Purtova, N. (2018). The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology, 10*(1), 48–49

[331] Skiljic, A. (2021, March 19). The status quo of health data inferences. *iapp.org*. Recruited from: https://iapp.org/news/a/the-statusquo-of-health-data-inferences/

[332] De Conca, S. (2021). *The enchanted house: An analysis of the interaction of intelligent personal home assistants (IPHAs) with the private sphere and its legal protection* (pp. 116).

[333] *See generally* De Conca, S. (2021). *The enchanted house: An analysis of the interaction of intelligent personal home assistants (IPHAs) with the private sphere and its legal protection*.

[334] Information can take many forms, such as alphabetic, numeric, video, or images, and the increasing prevalence of big data and data extraction technologies means that the definition of personal data is becoming more unstable over time. *See* Saglam, R. B., Nurse, J. R., & Hodges, D. (2022). Personal information: Perceptions, types and evolution. *Journal of Information Security and Applications*, *66*, 103163. *Also see* Purtova, N. (2020). Code as personal data. *INFO-LEG* [working paper], 5.

[335] *See generally* Dalla Corte, L. (2020). Safeguarding Data Protection in an Open Data World: On the idea of balancing open data and data protection in the development.

[336] As the distinction between various regulations in the EU for personal and non-personal data becomes increasingly evident, the idea that "data is a thing" is gaining prominence. However, any framework for data must acknowledge that data cannot solely be viewed as an economic asset to be commoditized or a tool for exerting pressure on private entities. Rather, it is inherently connected to the individuals whose data it

as 'information is data + meaning', which relates to a natural person adopting an operational standard.[337] The fragmented and ambiguous concept of data in EU law, along with the growing trend of regulating data as a commodity, overlooks the intrinsic connection between personal data and its subjects.[338] The failure of the European legislator to distinguish between technical terminology and everyday usage can lead to confusion between the distinction of data and information, which in turn carries profound implications for safeguarding personal data.[339]

As previously discussed, the material scope of personal data is based on the ability to identify a person, but it is becoming increasingly complex to determine whether the set of information identifying a person should be considered personal data..[340] An identity consists of a mix of numbers and values that may relate to an individual, but the same data may be shared for various data processing activities by multiple decentralised data processors.[341] Drawing on this premise, personal identity cannot be isolated from data-driven technologies, as the relationship between personal and non-personal data precedes our interactions with the environment.[342] The fundamental premise is that the processing of personal data has an effect on natural persons, while the processing of non-personal data does not.[343] Personal information is transformed into data through digital presence, which is then used to construct personal profiles through datafication.[344] This process can cause problems, especially when information has meaning but does not relate to an individual.[345] Even if inferences are inaccurate, they can constitute 'any information', as the element itself does not require information to be accurate. The borders of the categories are interconnected and often beg the question of what types of data are included or excluded.[346] The concern is to what degree this premise is still sustainable in the smart city.

represents. *See* Ducuing, C. (2021). The regulation of 'data': a new trend in the legislation of the European Union? *KU Leuven*.

[337] Floridi, L. (2005). Is semantic information meaningful data?. *Philosophy and phenomenological research*, *70*(2), 351-370.

[338] Ducuing, C. (2021). The regulation of 'data': a new trend in the legislation of the European Union? *KU Leuven*.

[339] Janeček, V. (2018). Ownership of personal data in the Internet of Things. *Computer law & security review*, *34*(5), 1042.

[340] Finck, M., & Pallas, F. (2020). They who must not be identified—distinguishing personal from non-personal data under the GDPR. *International Data Privacy Law*, *10*(1), 11-36.

[341] Van Der Sloot, B. (2020). Regulating non-personal data in the age of Big Data. In *Health Data Privacy under the GDPR* (pp. 90). Routledge.

[342] Mai, J.-E. (2016). Big data privacy: The datafication of personal information. *The Information Society, 32*(3), 192–199.

[343] Van der Sloot, B., Van Schendel, S., & López, C. A. F. (2022). The influence of (technical) developments on the concept of personal data in relation to the GDPR. *TILT – Tilburg Institute of Law, Technology, and Society*, 17.

[344] Søe, S. O., Jørgensen, R. F., & Mai, J. E. (2021). What is the 'personal' in 'personal information'?. *Ethics and Information Technology*, *23*(4), 630.

[345] Galič, M. (2019). Surveillance, privacy and public space in the Stratumseind Living Lab: The smart city debate, beyond data. *Ars Aequi, special issue July/August*.

[346] Solove, D. J. (2023). Data Is What Data Does: Regulating Use, Harm, and Risk Instead of Sensitive Data. *Harm, and Risk Instead of Sensitive Data* (pp. 31).

Contemporary data processing based on aggregated data can lead to notable individual and societal repercussions.[347]

Smart cities, such as the Stratumseind Living Lab, demonstrate potential issues with personal data, where the data processed evaluates and influences street behaviour.[348] The systems deployed in smart cities can determine human behaviour, and thus should be considered information relating to people in terms of effect.[349] The potential for secondary effects, deviations from original purposes, and the consideration of software as personal information are leading to data falling within the material scope of the GDPR.[350] This underscores the trend of continuously broadening the scope of personal information collection and usage, commonly known as 'data creep'.[351] The anticipated harm caused by extensive data processing is redefining the concept of personal data.[352] Regardless of whether the purpose is explicitly or implicitly stated, the danger of personal data being utilised for incompatible secondary purposes arises.[353] The algorithms and infrastructures employed in smart cities can convert any information into data, creating a significant challenge for the protection of personal data and its present understanding.[354]

One of the primary challenges with personal data in smart cities is its inherent instability.[355] As computing power and online connectivity continue to evolve, the amount of data being generated and processed increases, making it more likely for sensitive personal information to be inadvertently revealed.[356] The GDPR acknowledges that data can be incorrect and provides the data subject with the ability to correct it.[357] What is defined at the moment of *ex-ante processing* as personal data, will not

[347] Van der Sloot, B., Van Schendel, S., & López, C. A. F. (2022). The influence of (technical) developments on the concept of personal data in relation to the GDPR. *TILT – Tilburg Institute of Law, Technology, and Society*, 17.

[348] Galič, M., & Gellert, R. (2021). Data protection law beyond identifiability? Atmospheric profiles, nudging and the Stratumseind Living Lab. *Computer Law & Security Review*, *40*, 105486.

[349] Purtova, N. (2020). Code as personal data. *INFO-LEG* [working paper], 11.

[350] Purtova, N. (2020). Code as personal data. *INFO-LEG* [working paper], 1-14.

[351] Reidenberg, J. R. (1999). Resolving conflicting international data privacy rules in cyberspace. *Stanford Law Review*, *52*, 1315.

[352] Hildebrandt, M., & Tielemans, L. (2013). Data protection by design and technology neutral law. *Computer Law & Security Review*, *29*(5), 509-521.

[353] Koops, B. J. (2021). The concept of function creep. *Law, Innovation and Technology*, *13*(1), 47.

[354] Gellert, R. (2021). Personal data's ever-expanding scope in smart environments and possible path(s) for regulating emerging digital technologies. *International Data Privacy Law*, 11(2), 196–208.

[355] Janeček, V. (2018). Ownership of personal data in the Internet of Things. *Computer law & security review*, *34*(5), 1039-1052.

[356] Regulation 2016/679 of the European Parliament and of Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), O.J. (L 119), art. 4. *Also see* Quinn, P. (2021). The Difficulty of Defining Sensitive Data—The Concept of Sensitive Data in the EU Data Protection Framework. *German Law Journal*, 22(8), 1583-1612; Søe, S. O., Jørgensen, R. F., & Mai, J. E. (2021). What is the 'personal' in 'personal information'?. *Ethics and Information Technology*, *23*(4), 630.

[357] Articles 16 and 19 of the GDPR jo Recital 65 GDPR.

last and be confirmed at the moment of *ex-post processing* as non-personal and *vice-versa.*[358] In other words, a dataset or information may not be directly regarded as personal data at first sight but become personally identifiable at the end of the process (or through one of the intermediate processing phases).[359] The GDPR seems to disregard that data stages are not consistent and is thus fundamentally different from 'information'.[360] *De facto*, the GDPR fails to recognize the dynamic nature of data during its lifecycle, and this underscores the importance of clearly distinguishing between data and information to ensure effective protection of personal data in smart cities.[361]

5.2.3. Anonymous Data as a Failed Solution: Breaking Promises

The re-identification of data is important for data protection.[362] However, despite efforts to anonymize data, advances in data processing technology and the sheer volume of data available for analysis, are making absolute anonymity no longer achievable.[363] The distinction between personal and non-personal data is becoming increasingly dynamic and context-dependent,[364] making it difficult to determine whether a piece of data is truly anonymous.[365] This raises concerns about the effectiveness of current anonymization methods, particularly in light of the permeation of data-driven technologies and the

[358] For example, in the case of automatic processing of personal data, the Council of Europe has argued that even if based on an anonymous profile, the application of the profile to individuals entails that these individuals are *at least* identifiable, signifying that personal data is processed since the moment of collection. *See* Council of Europe (2010), The Protection of Individuals with Regard to Automatic Processing of Personal Data in the Context with Regard to Automatic Processing. *Recommendation CM/Rec(2010)13 and Explanatory Memorandum*, para 57. *See also* Galič, M., & Gellert, R. (2021). Data protection law beyond identifiability? Atmospheric profiles, nudging and the Stratumseind Living Lab. *Computer Law & Security Review*, *40*, 105486, 273.

[359] Koops, B. J. (2014). The trouble with European data protection law. *International data privacy law*, *4*(4), 250-261.

[360] Podda, E., & Palmirani, M. (2020). Inferring the Meaning of Non-personal, Anonymized, and Anonymous Data. In *AI Approaches to the Complexity of Legal Systems XI-XII* (pp. 269-282). Springer, Cham.

[361] Podda, E., & Palmirani, M. (2020). Inferring the Meaning of Non-personal, Anonymized, and Anonymous Data. In *AI Approaches to the Complexity of Legal Systems XI-XII* (pp. 269-282). Springer, Cham.

[362] Kröger, J. L. (2022). *Rogue Apps, Hidden Web Tracking and Ubiquitous Sensors* [Doctoral dissertation, Universität Berlin], 227–229

[363] Based on recent research on this issue, it can be concluded that successfully anonymising data is practically impossible for any complex dataset. *See* Ohm, P. (2009). Broken promises of privacy: Responding to the surprising failure of anonymization. *UCL Law Review*, *57*, 1701-1777; Sweeney, L. (2000). Simple demographics often identify people uniquely. *Health (San Francisco)*, *671*(2000), 1-34; Schwartz, P. M., & Solove, D. J. (2011). The PII problem: Privacy and a new concept of personally identifiable information. *NYUL rev.*, *86*, 1814.

[364] *See* Commission, 'On the free flow of data …' 34; Commission, 'Proposal for a Regulation of the European Parliament and of the Council on a framework for the free flow of non-personal data in the European Union' COM (2017) 495 final; Purtova, N (2017). Do property rights in personal data make sense after the Big Data turn? Individual control and transparency. *Tilburg Law School Research Paper No. 2017/21*, 13–17.

[365] Finck, M., & Pallas, F. (2020). They who must not be identified—distinguishing personal from non-personal data under the GDPR. *International Data Privacy Law*, *10*(1), 11-36.

interlinkage of data sources.[366] The traditional approach of rendering data anonymously to avoid application of the GDPR is becoming obsolete, as technological progress allows for previously anonymous data to become personal.[367] This evolution of data dynamics, coupled with GDPR's inability to keep pace, leads to anonymous data as a failed solution to circumvent its application.[368] While the GDPR recommends the use of adequately anonymized data to avoid regulation, techniques, such as data analytics and AI, can extract previously unknown information from large databases, making it clear that considering anonymous data as outside the scope of data protection law is a false sense of security.[369] Anonymous data can become personal data again, depending on future data linkages and technological developments.[370] Furthermore, the absence of a temporal restriction in the GDPR with regard to the re-identification or anonymization of data implies a high probability that the data will ultimately be linked to a natural person, rendering it as personal data.[371]

Merely anonymizing data is no longer sufficient to comply with the material scope of EU data protection law, regardless of personal data.[372] The *death of anonymization* and the challenges posed by smart cities to personal data highlight the need for a more nuanced and dynamic approach to defining and protecting personal data in the digital age.[373] To ensure the protection of personal data, the margins of what constitutes personal data should be clearly defined, and encryption and anonymization procedures should correspond to reality.[374] The reliance on anonymization as an absolute protection measure is inadequate and its effectiveness should be subjected to continuous re-evaluation and

[366] Kröger, J. (2019). Unexpected Inferences from Sensor Data: A Hidden Privacy Threat in the Internet of Things. In L. Strous and V. G. Cerf *(*Eds.), *Internet of Things. Information Processing in an Increasingly Connected World* (pp. 147–159)*.* Cham: Springer.

[367] As emphasised in Recital 9 of the Regulation on a framework for the free flow of non-personal data in the EU (FFDR) "if technological developments make it possible to turn anonymized data into personal data, such data are to be treated as personal data, and Regulation (EU) 2016/679 is to apply accordingly", Recital 9 of the framework for the free flow of non-personal data in the European Union. *See also* Podda, E. (2021) Shedding light on the legal approach to aggregate data under the GDPR & the FFDR [CONFERENCE OF EUROPEAN STATISTICIANS - Expert Meeting on Statistical Data Confidentiality]. *UNEC*. Retrieved on 22 November 2022 from https://unece.org/sites/default/files/2021-12/SDC2021_Day1_Podda_AD.pdf

[368] Ohm, P. (2009). Broken promises of privacy: Responding to the surprising failure of anonymization. *UCLA l. Rev.*, *57*, 1701.

[369] Purtova, N. (2018). The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, *10*(1), 40-81.

[370] Politou, E., Alepis, E., & Patsakis, C. (2018). Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions. *Journal of cybersecurity*, *4*(1), 3.

[371] Graef, I., & van der Sloot, B. (2022). Collective data harms at the crossroads of data protection and competition law: Moving beyond individual empowerment. *European Business Law Review*, *33*(4), 513-536.

[372] Dalla Corte, L. (2020). Safeguarding Data Protection in an Open Data World: On the idea of balancing open data and data protection in the development, 265.

[373] Kröger, J. L. (2022). *Rogue Apps, Hidden Web Tracking and Ubiquitous Sensors* [Doctoral dissertation, Universität Berlin], 227–229; Politou, E., Alepis, E., & Patsakis, C. (2018). Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions. *Journal of cybersecurity*, *4*(1), 3.

[374] Stalla-Bourdillon, S., & Knight, A. (2016). Anonymous data v. personal data-false debate: an EU perspective on anonymization, pseudonymization and personal data. *Wisconsin International Law, 34*, 284.

scrutiny.[375] As technological capabilities for de-anonymization improve, periodic reviews of technical standards for anonymizing data may be necessary.[376] This will ensure that the GDPR remains valid as a meaningful and economical exercise in regulating personal data.

5.3. The Paradoxical Loss of Control in the Smart City

The GDPR is designed to provide the highest level of legal protection for personal data and to ensure that individuals have control over their information.[377] However, the evolving nature of data protection has changed the traditional scenario of control and protection.[378] The blurring of boundaries between private, social, and public contexts challenges the idea that individuals have complete control over their personal data.[379] The increasing fluidity of personal data and the size of databases make it well nigh impossible for individuals to be aware of all data processing activities and to assess their legitimacy.[380] It may no longer be feasible to provide individuals with complete control over their personal data in these complex and interconnected environments.[381] In the smart city, characterised by the ubiquitous role of data processing technologies, comprehending the fate of personal information has become an arduous task, while the capacity of individuals to make informed decisions regarding their data is being

[375] Ohm, P. (2009). Broken promises of privacy: Responding to the surprising failure of anonymization. *UCLA l. Rev.*, *57*, 1701.

[376] The most technically sound approach to data anonymization is a contextual one. Technical experts generally reject the notion of complete or absolute anonymity and instead propose a continuum that measures the difficulty of de-anonymizing or re-identifying a dataset. Given this context, a binary classification of data as anonymous or non-anonymous is insufficient. Instead, it may be more appropriate to apply data protection standards proportionally to the level of anonymity achieved. Determining reasonably probable resources for de-anonymization is a critical factor in this approach, although this legal concept is often absent from technical discussions and lacks an exhaustive list of factors to consider.

[377] Purtova, N. (2018). The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, *10*(1), 41.

[378] De Conca, S. (2021). *The enchanted house: An analysis of the interaction of intelligent personal home assistants (IPHAs) with the private sphere and its legal protection* (pp. 122).

[379] See the WP29 ('WP207') on how the disclosure of public-sector information impacts the assessment of the 'other person' who may re-identify the data subject: "once data are publicly released for reuse, there will be no control over who can access the data. The likelihood that 'any other person' will have the means and will use those means to re-identify the data subjects will increase very significantly. Therefore, and irrespective of the interpretation of Recital 26 in other contexts, when it comes to making data available for reuse […] utmost care should be taken to ensure that the datasets to be disclosed should not include data that can be re-identified by means likely reasonably to be used by any person, including potential re-users, but also other parties that may have an interest in obtaining the data, including law enforcement'. *See* WP29, Opinion 06/2013 on Open Data and Public Sector Information ('PSI') *Reuse WP207*, 13. *See also* Narayanan, A., & Shmatikov, V. (2010). Myths and fallacies of" personally identifiable information". *Communications of the ACM*, *53*(6), 24-26.

[380] Lazaro, C., & Metayer, D. L. (2015). Control over personal data: True remedy or fairy tale. *SCRIPTed*, *12*, 3.

[381] Geradin, D., Karanikioti, T., & Katsifis, D. (2021). GDPR Myopia: how a well-intended regulation ended up favouring large online platforms-the case of ad tech. *European Competition Journal*, *17*(1), 47-92.

subverted by the very technology that is supposed to protect them.[382] The prevailing emphasis on the legality of data processing, rather than the ethical and appropriate use of personal data, tends to distract us from the more pressing concerns in this domain.[383]

The notion of control in the GDPR is becoming ambiguous and difficult to enforce as data protection laws are unable to keep up with real-time and continuous profiling in smart environments.[384] The reliance on control raises two questions about *what* is being controlled and *who* is controlling it.[385] Furthermore, technology exerts a significant influence on an individual's behaviour and social interactions, and the GDPR may not fully comprehend the power dynamics and control concerns associated with technology.[386] In fact, technology may possess a volition of its own, beyond human control, or as Koops contends, "what kind of world do individuals inhabit who assert that they can exercise authority over their personal data?".[387] The rationale of technological infrastructure establishes the definition of personal data, and both society and individuals rely on this infrastructure. In the context of smart cities, control over personal data becomes dependent on the technology used, resulting in an affordance that is almost impossible to control.[388] The presence of information asymmetry between the agents utilising technology in the smart city and the individuals who unwittingly or knowingly share their data engenders a paradoxical situation in relation to the status of personal data, which ultimately challenges the notion of control.[389]

5.4. Conclusion

This chapter examines the challenges associated with applying the concept of personal data in the context of smart cities. The paradox of personal data in this context arises from the tension between the growing collection and processing of personal data and the need for individuals to maintain control over

[382] Moerel, L. (2014). Big Data Protection. How to Make the Draft EU Regulation on Data Protection Future Proof. How to Make the Draft EU Regulation on Data Protection Future Proof. *Tilburg Institute for Law, Technology, and Society.*

[383] Jastroch, N. (2020). Trusted artificial intelligence: on the use of private data. In *Product Lifecycle Management Enabling Smart X: 17th IFIP WG 5.1 International Conference, PLM 2020, Rapperswil, Switzerland, July 5–8, 2020, Revised Selected Papers 17* (pp. 659-670). Springer International Publishing.

[384] Irti, C. (2022). Personal Data, Non-personal Data, Anonymised Data, Pseudonymised Data, De-identified Data. In *Privacy and Data Protection in Software Services* (p. 53). Springer, Singapore.

[385] Taylor, L., Floridi, L., & Van Der Sloot, B. (2017). Introduction: a new perspective on privacy. In L. Taylor, L., Floridi & B. Van Der Sloot (Eds.). *Group privacy: New challenges of data technologies* (Vol. 126).

[386] Lazaro, C., & Metayer, D. L. (2015). Control over personal data: True remedy or fairy tale. *SCRIPTed*, *12*, 3.

[387] Koops, B. J. (2014). The trouble with European data protection law. *International data privacy law*, *4*(4), 250-261.

[388] McDonald, A. M., & Cranor, L. F. (2008). The cost of reading privacy policies. *Isjlp*, *4*, 543; Dalla Corte, L. (2020). Safeguarding Data Protection in an Open Data World: On the idea of balancing open data and data protection in the development, 53.

[389] Waerdt, van de, P. (2020). Information asymmetries: recognizing the limits of the GDPR on the data-driven market. Computer Law & Security Review, 38, [105436], 14.

their (personal) information. Determining what data falls into the category of ‘personal’ data and maintaining control over it poses significant challenges due to the expanding amount of data considered personal resulting from the proliferation of data. The classification of data is no longer solely determined by inherent dataset characteristics, but the efforts of the controller also influence it. The GDPR’s dependence on the concept of personal data as an operational tool is problematic because of the absence of a clear boundary-marker, which allows nearly any data to be classified as personal.[390] In smart cities, where every aspect of the environment and individuals is transformed into data, it becomes challenging to maintain a coherent definition of personal data as data is inevitably linked to individuals. Legal categories of data have become more ambiguous and dynamic, resulting in varying interpretations by different parties. Consequently, any form of personal data processing, no matter how minor or ordinary it may seem, falls within the scope of the GDPR.[391] In order to reconcile the legal framework with the technical reality of smart cities, a more sophisticated approach is required. The aim of this is to acknowledge the intricate nature of data sharing and personal data protection in such environments. To ensure effective data protection, individuals must possess a comprehensive comprehension of the data that is being stored and its utilisation. Therefore, it is essential that the concept of personal data is unambiguous and practicable. The legal system must address the entire gamut of issues and present practical resolutions, rather than being embroiled in discussions surrounding the definition of personal data.

[390] Dalla Corte, L. (2020). Safeguarding Data Protection in an Open Data World: On the idea of balancing open data and data protection in the development, 244.

[391] Koops, B. J. (2014). The trouble with European data protection law. *International data privacy law*, *4*(4), 250-261.

Chapter VI.

The Future of Personal Data in the Smart City: Navigating the Intersection of Technology and Data Protection

The success of smart cities, as well as the future of personal data protection, depends on the synergy between law and technology.[392] The availability of data is fundamental to the successful utilisation of the smart city. With the advancement of technology and the ever-increasing capabilities of data processing, it becomes more and more difficult to maintain the current definition of personal data under the existing framework, thereby jeopardising the protection of personal data in the future. To overcome the futility of the concept of personal data, the smart city warrants a careful scrutiny of the implementation of data protection with the underlying technology. This chapter aims to reconcile the growing availability of data in smart cities with the right to personal data protection by developing future-proof recommendations so the validity of the concept of personal data stands the test of real-life settings.

6.1. Redefining Personal Data: Navigating the Legal Implications of Personal Data in the Smart City

The GDPR needs to be revised to address the widespread emergence of new technologies to ensure it remains relevant, effective, and sustainable in safeguarding personal data.[393] The current definition blends together different types of personal data, leading to an overloaded system with an unclear comprehension of what qualifies as personal data and what does not.[394] To resolve this matter, a comprehensive and durable interpretation that incorporates multidisciplinary perspectives,

[392] Galič, M., & Gellert, R. (2021). Data protection law beyond identifiability? Atmospheric profiles, nudging and the Stratumseind Living Lab. *Computer Law & Security Review*, *40*, 105486.

[393] As argued by Axel Voss, one of the fathers of the General Data Protection Regulation. *See* Espinoza, J (2021, March 4). EU data protection laws need overhaul, says policy architect; GDPR. *Financial Times (London, England).* Retrieved from https://advance-lexis-com.vu-nl.idm.oclc.org/api/document?collection=news&id=urn:contentItem:624G-V5C1-DYTY-C3DR-00000-00&context=1516831. *See also* Van Lieshout, M. (2016). Privacy and Innovation: From Disruption to Opportunities. *Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection*, 195-212.

[394] Purtova, N. (2018). The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, *10*(1), 40-81

encompassing both fundamental and sophisticated legal and technical expertise is proposed.[395] While the use of personal data is crucial for the development of well-functioning smart cities, it must be subject to conditions that ensure the effective protection of individuals' (data protection) rights.[396] The GDPR is technology-neutral and focuses on the effects rather than the means, aiming to regulate the use of technology without hindering its development.[397] However, the active interpretation of the legislation plays a crucial role in determining the scope of protection.[398] It may not be desirable to impose the same level of protection on all data processing since data-processing algorithms attach meaning to personal data differently from human interpretation.[399] Instead, the focus should be on the potential harm that the technology used could cause to individuals. By adopting a more specific and sustainable interpretation of the definition of personal data, individuals' data protection rights in smart cities can be strengthened. Such an interpretation would provide a clearer understanding of what types of data are considered personal and require protection.[400]

Additionally, while the principle of data minimization and data protection by design are already established within the framework of the GDPR, there is a need for greater emphasis on the implementation in practice.[401] It is crucial to uphold and enforce data protection by design, considering the privacy implications of data collection, processing, and sharing from the outset and taking steps to minimise the amount of personal data that is collected and shared. This approach would ensure that only the data that is truly necessary for the functioning of smart cities is collected and used, and that all other data is kept to a minimum.[402] Finally, data protection laws should be adapted to reflect the changing nature of data in a smart city context. For example, laws could be updated to address the challenges posed by new technologies that can collect, process, and analyse vast amounts of personal data in real-time. New provisions could be added to ensure that data collected by smart city technologies is used in

[395] Solove, D. J. (2023). Data Is What Data Does: Regulating Use, Harm, and Risk Instead of Sensitive Data. *Harm, and Risk Instead of Sensitive Data* (pp. 43).

[396] Purtova, N. (2018). The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, *10*(1), 78-79.

[397] Koops, E. J. (2006). Should ICT Regulation Be Technology-Neutral? In B. J. Koops, A. M. B. Lips, J. E. J. Prins, & M. H. M. Schellekens (Eds.), *Starting Points for ICT Regulation* (pp. 82-85). (Information Technology and Law Series, No. 9). The Hague: T.M.C. Asser Press.

[398] Purtova, N. (2018). The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, *10*(1), 78-79.

[399] Hildebrandt, M. (2013). Slaves to Big Data. Or are we?. *IDP Revista De Internet, Derecho Y Política,* 16.

[400] Zangrandi, R. (n.d.) I'm sorry my Friend, but you're Implicit in the Algorithm. Privacy and Internal Access to Big Data Stream: An Interview with Giovanni Buttarelli. *European Data Protection Supervisor.* Retrieved from https://edps.europa.eu/data-protection/our-work/publications/articles/%E2%80%98i%E2%80%99m-sorry-my-friend-you%E2%80%99re-implicit-algorithm%E2%80%A6%E2%80%99_en

[401] Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation'), Article 5(1)(c) GDPR. Article 25 GDPR for data protection by design and by default and Recital 78 GDPR on appropriate Technical and Organisational Measures.

[402] Koops, E. J. (2006). Should ICT Regulation Be Technology-Neutral? In B. J. Koops, A. M. B. Lips, J. E. J. Prins, & M. H. M. Schellekens (Eds.), *Starting Points for ICT Regulation* (pp. 82-85). (Information Technology and Law Series, No. 9). The Hague: T.M.C. Asser Press.

a way that is transparent, secure, and respectful of individuals' rights. It is important to engage in interdisciplinary collaboration between the technology and legal fields, as well as to engage in continuous dialogue between the relevant parties to ensure that the legal framework remains relevant and effective in safeguarding the concept.[403]

6.1.1. A New Approach: The Realistic Risks and Harms of Personal Data

The concept of personal data fails to capture the diverse means by which personal information can be gathered and exploited within smart environments, and it indiscriminately extends the same degree of safeguarding to all information that qualifies as personal.[404] To address these issues, a more effective approach would be to consider the potential risks and harms that data processing can cause,[405] rather than solely relying on the nature of the data.[406] In the context of smart cities, where technology is capable of perceiving the environment and acting upon the environment, it is essential to assume that all data potentially has meaning.[407] While certain types of personal data are not inherently harmful, they can become harmful or create a risk of harm when they are used in certain ways.[408] Therefore, the concept

[403] Purtova, N. (2018). The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, *10*(1), 53; Solove, D. J. (2023). Data Is What Data Does: Regulating Use, Harm, and Risk Instead of Sensitive Data. *Harm, and Risk Instead of Sensitive Data (pp. 43)*; Van der Sloot, B., & van Schendel, S. (2021). Procedural law for the data-driven society. *Information & Communications Technology Law*, *30*(3), 304-332.

[404] Providing a comprehensive answer to the question "in which ways can personal data be used against the data subject?", *see* Kröger, J. L., Miceli, M., & Müller, F. (2021). How data can be used against people: a classification of personal data misuses [Preprint]. *Available at SSRN 3887097,* 9.

[405] Solove, D. J. (2023). Data Is What Data Does: Regulating Use, Harm, and Risk Instead of Sensitive Data. *Harm, and Risk Instead of Sensitive Data (pp. 43)*; Van der Sloot, B., & van Schendel, S. (2021). Procedural law for the data-driven society. *Information & Communications Technology Law*, *30*(3), 304-332.

[406] Van der Sloot, B., & van Schendel, S. (2021). Procedural law for the data-driven society. *Information & Communications Technology Law*, *30*(3), 304-332.

[407] Purtova, N. (2018). The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, *10*(1), 53.

[408] The classification of harms is meant to be universally applicable, independent of how the data was obtained (e.g., online or offline, legally or illegally, collected or inferred, with or without the knowledge of the data subject), who causes the threat (e.g., individual person, corporation organised crime group, intelligence agency) and what motivations lie behind it (e.g., financial gain, political objectives,revenge). Similarly, it has been appointed by experts that the use of certain data categories for certain purposes (e.g., personalised pricing, credit/insurance scoring, targeted advertising) should be prohibited because the expected societal benefits do not outweigh the costs and risks involved. For instance, Solove proposes "hard boundaries that block particularly troublesome practices", *see* f Solove, D. J. (2012). Introduction: Privacy self-management and the consent dilemma. *Harvard Law Review 1*, *126*, 1903. For a more detailed analysis on classifications of games, *see* Kröger, J. L., Miceli, M., & Müller, F. (2021). How data can be used against people: a classification of personal data misuses [Preprint]. *Available at SSRN 3887097*; Solove, D. J. (2023). Data Is What Data Does: Regulating Use, Harm, and Risk Instead of Sensitive Data. *Harm, and Risk Instead of Sensitive Data.*

of personal data should stress the misuse of personal data to provide a comprehensive and clear overview of potential paths of harm.[409]

A proposed classification of personal data should apply to any information that is or once was personal data, including anonymized data, as long as it has the potential to cause or facilitate harm against the data subject.[410] This would allow for a clearer threshold of protection based on the risk of identification, as opposed to the current approach, which applies the full range of GDPR requirements to all information deemed to be personal data.[411] The application of data protection law should be based on the potential negative consequences of each data processing on the rights and freedoms of individuals, regardless of whether the data processed qualifies as personal.[412] To gain a more comprehensive understanding of potential harm and avoid overlooking paths of harm in impact assessments and public discourse, it is necessary to implement a risk-based approach to interpreting personal data.[413] Such an approach would enable regulators to tailor their protection measures based on the level of risk posed by different types of data.[414] A promising way forward is to shift the focus away from possible identification and towards providing guidance on different risk profiles, particularly given the potential for de-identified data to cause harm.[415]

In order to ensure effective protection of personal data, the definition of personal data must be revised to reflect the realistic risk of identification, taking into account the social, economic, and political contexts in which the data is generated, as well as the technological environment and potential threats surrounding the data.[416] This revision should involve the classification of data into distinct types and the establishment of different levels of protection for each type. While browsing history and purchase history may not directly identify individuals, they can reveal sensitive information about their

[409] Kröger, J. L., Miceli, M., & Müller, F. (2021). How data can be used against people: a classification of personal data misuses [Preprint]. *Available at SSRN 3887097*; Solove, D. J. (2023). Data Is What Data Does: Regulating Use, Harm, and Risk Instead of Sensitive Data. *Harm, and Risk Instead of Sensitive Data (pp. 43).*

[410] Kröger, J. L., Miceli, M., & Müller, F. (2021). How data can be used against people: a classification of personal data misuses [Preprint]. *Available at SSRN 3887097,* 3.

[411] Kröger, J. L., Miceli, M., & Müller, F. (2021). How data can be used against people: a classification of personal data misuses [Preprint]. *Available at SSRN 3887097*; Solove, D. J. (2023). Data Is What Data Does: Regulating Use, Harm, and Risk Instead of Sensitive Data. *Harm, and Risk Instead of Sensitive Data (pp. 43).*

[412] Galič, M., & Gellert, R. (2021). Data protection law beyond identifiability? Atmospheric profiles, nudging and the Stratumseind Living Lab. *Computer Law & Security Review*, *40*, 105486.

[413] Harm involves negative consequences from the use of personal data that affect individuals or society. Risk involves the likelihood and gravity of certain harms that have not yet occurred. Such as, discrimination, unfairness, and exclusion, regardless of whether the data is personal or non-personal. *See* Solove, D. J. (2023). Data Is What Data Does: Regulating Use, Harm, and Risk Instead of Sensitive Data. *Harm, and Risk Instead of Sensitive Data* (pp. 43). *See also* Omotubora, A., & Basu, S. (2020). Next generation privacy. *Information & Communications Technology Law*, *29*(2), 169.

[414] Solove, D. J. (2023). Data Is What Data Does: Regulating Use, Harm, and Risk Instead of Sensitive Data. *Harm, and Risk Instead of Sensitive Data* (pp. 31).

[415] Hintze, M. (2018). Viewing the GDPR through a de-identification lens: a tool for compliance, clarification, and consistency. *International Data Privacy Law*, *8*(1), 86-101.

[416] Schwartz, P. M., & Solove, D. J. (2011). The PII problem: Privacy and a new concept of personally identifiable information. *NYUL rev.*, *86*, 1814.

preferences, habits, and lifestyles, and are often used to create targeted advertising that can significantly impact consumer behaviour and decision-making.[417] Therefore, a risk-based approach to data protection should not solely rely on the uniqueness of personal data but also consider the potential harms that could arise from the (mis)use.[418] Furthermore, data directly linked to an individual, such as their name, address, and social security number, should be considered highly sensitive and require a higher level of protection.[419] Data that is less uniquely identifiable to an individual, such as browsing history or purchase history, could be deemed less sensitive and may require a lower level of protection. However, it is essential to consider the potential harm that can result from the misuse or mishandling of personal data, regardless of whether it is easily identifiable or not. In some cases, non-identifiable data may be more vulnerable to abuse, as it may be more easily accessible or shared without proper consent.[420] Therefore, a risk-based approach should be used to assess the level of protection required for different types of personal data, taking into account not only the identifiability of the data but also the potential harms that may arise from its processing.[421] This approach would provide a clearer threshold of protection based on the risk of identification, rather than applying the full range of GDPR requirements to all information deemed to be personal data.[422] By taking a more holistic view of the problem and considering both subjective and objective risks, potential paths of harm can be addressed and overlooked in impact assessments and public discourse.[423] This multidisciplinary approach would promote a more sustainable and effective interpretation and application of Article 4(1) of the GDPR in the context of smart cities and the protection of personal data.[424]

[417] Omotubora, A., & Basu, S. (2020). Next generation privacy. *Information & Communications Technology Law*, *29*(2), 169.

[418] *See generally* Solove, D. J. (2023). Data Is What Data Does: Regulating Use, Harm, and Risk Instead of Sensitive Data. *Harm, and Risk Instead of Sensitive Data.*

[419] Solove, D. J. (2023). Data Is What Data Does: Regulating Use, Harm, and Risk Instead of Sensitive Data. *Harm, and Risk Instead of Sensitive Data (pp. 43)*; Van der Sloot, B., & van Schendel, S. (2021). Procedural law for the data-driven society. *Information & Communications Technology Law*, *30*(3), 304-332.

[420] Finck, M., & Pallas, F. (2020). They who must not be identified—distinguishing personal from non-personal data under the GDPR. *International Data Privacy Law*, *10*(1), 11-36.

[421] Solove, D. J. (2023). Data Is What Data Does: Regulating Use, Harm, and Risk Instead of Sensitive Data. *Harm, and Risk Instead of Sensitive Data (pp. 43).*

[422] Hon, W. K., Millard, C., & Walden, I. (2011). The problem of 'personal data' in cloud computing: what information is regulated?—the cloud of unknowing. *International Data Privacy Law*, *1*(4), 211-228.

[423] Solove, D. J. (2023). Data Is What Data Does: Regulating Use, Harm, and Risk Instead of Sensitive Data. *Harm, and Risk Instead of Sensitive Data* (pp. 8).

[424] Impact assessments are already an established tool in the GDPR (e.g., "data protection impact assessment", Art. 35 GDPR) but, thus far, they are mainly conducted by the data controllers themselves, which can obviously entail significant conflicts of interest. Two recent EU initiatives towards a stronger risk-based government regulation of data use are the proposed AI Act, under which artificial intelligence applications could face special requirements or even a legal prohibition based on their estimated harm potential (European Commission 2021), and the proposed Digital Services Act, which could include restrictions on profiling-based advertising. These initiatives are interesting, but their real impact remains to be seen and depends, of course, on the final legislative outcome and the rigour of enforcement. *See* Kröger, J. L. (2022). *Rogue Apps, Hidden Web Tracking and Ubiquitous Sensors* [Doctoral dissertation, Universität Berlin], 227–229. *Also see* Omotubora, A., & Basu, S. (2020). Next generation privacy. *Information & Communications Technology Law*, *29*(2), 169-170.

In a world with rapidly evolving technology, the distinction between personal data and non-personal data is becoming less relevant .[425] As argued by Purtova, in circumstances where personal data covers everything, "we should abandon the distinction between personal and non-personal data, embrace the principle that all data processing should trigger protection, and understand how this protection can be scalable".[426] In the context of smart city technologies, it is imperative to prioritise the appropriateness of data processing and to strike a balance between the interests of the collective and the individual.[427] This approach entails evaluating the risk of identification and offers a more technically sound method of protecting personal data by emphasising the technical aspects of smart environments and acknowledging the data lifecycle.[428] Personal data is not a static concept, but rather dynamic, and its level of identifiability varies on a spectrum of risk that changes over time with changing conditions.[429] Smart technologies allow for real-time identification or re-identification of individuals, leading to new forms of identifiability and corresponding obligations on data controllers and processors across various smart settings.[430] It is important to note that not all data processing poses an equal level of risk or intrusion, and thus, not all data should not be treated equally.[431] To safeguard individuals' personal data and mitigate risks, it is essential to differentiate between various types of data.[432] Therefore, it is imperative to consider the technical capabilities and potential intentions of data controllers when developing appropriate technical, organisational, and regulatory measures and assessing potential harms associated with data collection and the use of smart technologies.[433] The complexity of smart technologies presents new challenges for personal data protection, but it also offers opportunities to redefine the discourse on the reconstruction of personal data.[434]

[425] Weitzenboeck, E. M., Lison, P., Cyndecka, M., & Langford, M. (2022). The GDPR and unstructured data: is anonymization possible?. *International Data Privacy Law*, *12*(3), 184-206.

[426] Purtova, N. (2018). The Law of Everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, *10*(1), 40.

[427] Moiny, J. P., De Terwangne , C., Van Gyseghem, J-M., & Poullet, Y. (2010). *Rapport sur les lacunes de la Convention n° 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel face aux développements technologiques (Partie II)*. Conseil de l'Europe.

[428] Van Der Sloot, B. (2020). Regulating non-personal data in the age of Big Data. In *Health Data Privacy under the GDPR* (pp. 97). Routledge.

[429] Solove, D. J. (2023). Data Is What Data Does: Regulating Use, Harm, and Risk Instead of Sensitive Data. *Harm, and Risk Instead of Sensitive Data* (pp. 8).

[430] Omotubora, A., & Basu, S. (2020). Next generation privacy. *Information & Communications Technology Law*, *29*(2), 170.

[431] Omotubora, A., & Basu, S. (2020). Next generation privacy. *Information & Communications Technology Law*, *29*(2), 170.

[432] Omotubora, A., & Basu, S. (2020). Next generation privacy. *Information & Communications Technology Law*, *29*(2), 170.

[433] Purtova, N. (2018). The Law of Everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, *10*(1), 40; Weitzenboeck, E. M., Lison, P., Cyndecka, M., & Langford, M. (2022). The GDPR and unstructured data: is anonymization possible?. *International Data Privacy Law*, *12*(3), 184-206.

[434] However, the question remains of how we know where to draw the boundaries between the compliance regimes of different intensity, and how we know a particular configuration will meet the protective objectives of

In order to ensure adequate and sustainable protection of personal data in the context of emerging technologies such as smart cities, it is important to shift the focus away from solely classifying data as 'personal' and instead consider the potential harms that may result from its use.[435] The updated definition should account for the potential risks associated with the processing of personal data, such as, profiling, discrimination, and manipulation.[436] This will ensure that the GDPR is adapted to reflect the changing realities of data-driven environments, such as smart cities, and remain effective in providing suitable protection for personal data.[437] To address these challenges, it is suggested to preserve the broad interpretation of personal data but that compliance obligations be scaled according to the level of risk.[438] Achieving perfect data protection is not feasible, nor is it necessarily desirable. Rather, the level of protection should begin with acknowledging that there may always be some residual risk of identification.[439] To effectively address harms, the law should not be limited to the specific type of personal data being used, but instead should focus on how the data is being used.[440]

6.1.2. Updating the Elements of 'Identifiability' and 'Relating to' in the Smart City

The law should not protect personal data for its own sake.[441] The current approach to personal data protection is flawed because it prioritises the type of data over how it is used, leading to an arbitrary

the data protection law? *See* Purtova, N. (2018). The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology, 10*(1), 40-81.

[435] Kröger, J. L., Miceli, M., & Müller, F. (2021). How data can be used against people: a classification of personal data misuses [Preprint]. *Available at SSRN 3887097,* 10.

[436] Profiling involves the use of automated means to analyse personal data and create a profile of an individual. Discrimination occurs when personal data is used to make decisions based on characteristics such as race, ethnicity, or gender. Manipulation involves the use of personal data to influence an individual's behaviour or decisions. Notably, while the risks of data have the potential to be ethically indefensible and cause harm, depending on the context and intentions, some of the data uses can benefit both the data subject and society. *See* Kröger, J. L., Miceli, M., & Müller, F. (2021). How data can be used against people: a classification of personal data misuses [Preprint]. *Available at SSRN 3887097,* 10.

[437] European Commission. (2010). Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Youth Opportunities Initiative: 'A comprehensive approach on personal data protection in the European Union'. *COM(2010) 609 final*. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0609:FIN:EN:PDF

[438] Koops proposed different sets of obligations for different kinds of personal data to an improvement on the compliance regime under the GDPR. Due to the scope of this thesis, this suggestion will not be further elaborated on. *See* Koops, B. J. (2014). The trouble with European data protection law. *International data privacy law*, *4*(4), 250-261. *Also see* Purtova, N. (2018). The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology,* 10(1), 79.

[439] Finck, M., & Pallas, F. (2020). They who must not be identified—distinguishing personal from non-personal data under the GDPR. *International Data Privacy Law*, *10*(1), 35.

[440] Such as the proposed specific harms and risks that may arise from the use of personal data. *See* Van Der Sloot, B. (2017). *Privacy as virtue* (pp. 154). Intersentia.

[441] Solove, D. J. (2023). Data Is What Data Does: Regulating Use, Harm, and Risk Instead of Sensitive Data. *Harm, and Risk Instead of Sensitive Data* (pp. 43).

and subjective definition of personal data.[442] This issue is compounded in smart environments, where all data stored, processed, and analysed have the potential to identify residents.[443] Therefore, the concept of personal data needs to be re-evaluated to include new types of data generated by smart devices and sensors, such as biometric and geo data, that uniquely tie to an individual and can be used to identify or track them.[444] The elements of 'identifiability' and 'relating to' should be expanded to encompass these new types of data, but the protection of personal data should be proportional to the outcome and consider the varying forms of the connection between information and a person.[445]

To address the challenges posed by the new landscape, a dynamic approach to data protection is required,[446] focusing on the processing of personal data rather than distinguishing between personal and non-personal data.[447] The use of data, the activities, and the purposes and effects of those activities should be considered to determine appropriate regulations that comply with the legal framework.[448] Information security could help define the relationship between information and individuals,[449] and prevent unauthorised and inappropriate access to data.[450] Technology tends to respond better to information security.[451] Information security focuses on technical requirements stemming from the

[442] Solove, D. J. (2023). Data Is What Data Does: Regulating Use, Harm, and Risk Instead of Sensitive Data. *Harm, and Risk Instead of Sensitive Data* (pp. 45-48).

[443] Dalla Corte, L. (2019). Scoping personal data: towards a nuanced interpretation of the material scope of EU data protection law. *European Journal of Law and Technology*, *10*(1).

[444] Schwartz, P. M., & Solove, D. J. (2011). The PII problem: Privacy and a new concept of personally identifiable information. *NYUL rev.*, *86*, 1814.

[445] Solove, D. J. (2023). Data Is What Data Does: Regulating Use, Harm, and Risk Instead of Sensitive Data. *Harm, and Risk Instead of Sensitive Data* (pp. 43).

[446] Janeček, V. (2018). Ownership of personal data in the Internet of Things. *Computer law & security review*, *34*(5), 1039-1052.

[447] Søe, S. O., Jørgensen, R. F., & Mai, J. E. (2021). What is the 'personal' in 'personal information'?. *Ethics and Information Technology*, *23*(4), 628.

[448] Solove, D. J. (2023). Data Is What Data Does: Regulating Use, Harm, and Risk Instead of Sensitive Data. *Harm, and Risk Instead of Sensitive Data* (pp. 43).

[449] Information security could help with this. The general guidance documents such as the ISO guidelines on risk management could be a starting point for this. *See* International Organization for Standardization (2018, February) ISO 31000:2018 Risk management – Guidelines. (February 2018). Retrieved from https://www.iso.org/standard/65694.html
Also see Choenni, S., Bargh, M. S., Busker, T., & Netten, N. (2022). Data governance in smart cities: Challenges and solution directions. *Journal of Smart Cities and Society*, 1-21.

[450] For instance, recently a new cybersecurity paradigm called zero-trust has emerged as a promising solution to protect such information systems. The Dutch National Cyber Security Centre in a recent report has advised organisations to deploy the zero-trust model in their future investments. For IoT based systems there are also a rising number of publications advocating the zero-trust model to protect these systems, *see* Chen, Z., Yan, L., Lü, Z., Zhang, Y., Guo, Y., Liu, W., & Xuan, J. (2021). Research on zero-trust security protection technology of power IoT based on blockchain. In *Journal of Physics: Conference Series* (Vol. 1769, No. 1, p. 012039). IOP Publishing. *See also* Choenni, S., Bargh, M. S., Busker, T., & Netten, N. (2022). Data governance in smart cities: Challenges and solution directions. *Journal of Smart Cities and Society*, 1-21; Pan, J., & Yang, Z. (2018, March). Cybersecurity challenges and opportunities in the new "Edge Computing+ IoT" world. In *Proceedings of the 2018 ACM International Workshop on Security in Software Defined Networks & Network Function Virtualization* (pp. 29-32).

[451] Van Lieshout, M. (2016). Privacy and Innovation: From Disruption to Opportunities. *Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection*, 195-212.

treatment of personal data.[452] By interconnecting information security with the data protection discourse, a more nuanced and comprehensive understanding of the interpretation of information and data can be achieved, as well as the meaning of data and information in relation to technology and the concept of personal data.[453]

Furthermore, the definition of personal data encounters challenges, particularly when the two critical components, identifiability and relating to, interact and exacerbate the difficulties.[454] In smart environments, where all data stored, processed, and analysed have the potential, *inter alia*,[455] to identify the residents, the relationship between information and a person is more intricate.[456] Therefore, the concept of personal data in smart cities surpasses simple identifiability,[457] necessitating a profound understanding of the scope of identifiability and relating to, considering the novel types of data generated and utilised in these environments, and addressing the complexity of determining if a set of information constitutes personal data.[458] This includes expanding the identification element to encompass other data types such as biometric and geo data that can uniquely tie an individual and facilitate their identification or tracking.[459] Secondly, the relationship between information and the person can manifest in various forms, including information on the person's characteristics, preferences, behaviours, and activities,[460] which may require updating the definition of personal data in smart environments to include the new data generated by smart devices and sensors, such as data on the person's movements, habits, and routines.[461] However, the inclusion of these new data types should be proportional to the desired outcome and should consider the diverse forms the connection between information and a person can take.[462] The elements of identifiability and relating to should be expanded

[452] Stamp, M. (2011). *Information security: principles and practice* (pp. 2). John Wiley & Sons.

[453] Van Lieshout, M. (2016). Privacy and Innovation: From Disruption to Opportunities. *Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection*, 195-212.

[454] *See generally* Finck, M., & Pallas, F. (2020). They who must not be identified—distinguishing personal from non-personal data under the GDPR. *International Data Privacy Law*, *10*(1), 11-36.

[455] Dalla Corte, L. (2020). Safeguarding Data Protection in an Open Data World: On the idea of balancing open data and data protection in the development, 10.

[456] Hildebrandt, M. (2006). Profiling: From data to knowledge: The challenges of a crucial technology. *Datenschutz und Datensicherheit-DuD*, *30*(9), 550. *See also* Gellert, R. M. (2021). Personal data's ever-expanding scope in smart environments and possible path (s) for regulating emerging digital technologies. *International Data Privacy Law*, 11(2), 208.

[457] Purtova, N. (2018). The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, 10(1), 42.

[458] Leiser, M. R., & Dechesne, F. (2020). Governing machine-learning models: challenging the personal data presumption. *International Data Privacy Law, 10*(3), 187.

[459] Quach, S., Thaichon, P., Martin, K. D., Weaven, S., & Palmatier, R. W. (2022). Digital technologies: Tensions in privacy and data. *Journal of the Academy of Marketing Science*, *50*(6), 1299-1323.

[460] Purtova, N. (2018). The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology,* 10(1), 40-81.

[461] Dalla Corte, L. (2020). Safeguarding Data Protection in an Open Data World: On the idea of balancing open data and data protection in the development, 237.

[462] Purtova, N. (2020). Organising concepts in law: A typology and lessons for data protection. *NFO-LEG [working paper],* 15.

to accommodate the new data types unique to smart environments but within reasonable limits.[463] The potential broad scope of the link between data and personal information can be limited by considering its interaction with the identifiability requirement, especially when taking into account the lifecycle of personal data.[464] However, continual evaluation is crucial in the realm of personal data protection. The requirements and definition of personal data should undergo a process of ongoing ideation, iteration, and critique to assess their effectiveness and adaptability to changing circumstances. This active approach allows for a more responsive and dynamic system that can evolve with emerging technologies and new types of data.[465]

6.2. Aligning the Technical Reality with Data Protection

The definition of personal data has a conceptual error based on certain axioms.[466] Ensuring data protection in smart cities demands a comprehensive approach that transcends the purview of legal perspectives.[467] The interaction between law and technology is becoming more complex, highlighting a disconnection between the legal paradigm and data-driven applications.[468] While the law is designed to safeguard the individual's private interests, it often fails to address the complex problems that arise from large-scale data processing operations.[469] Smart cities, in particular, pose significant challenges to conventional conceptions of personal data due to the abundance of information they generate.[470] The GDPR is inadequate for managing data processed in smart environments, given that it is often interlinked, aggregated, and combined, rendering it challenging to anticipate its future use and impact on individuals.[471] Addressing individual-level infringements caused by data alone may neglect the root

[463] Finck, M., & Pallas, F. (2020). They who must not be identified—distinguishing personal from non-personal data under the GDPR. *International Data Privacy Law*, *10*(1), 35.

[464] Dalla Corte, L. (2019). Scoping personal data: towards a nuanced interpretation of the material scope of EU data protection law. *European Journal of Law and Technology*, *10*(1), 16.

[465] Finck, M., & Pallas, F. (2020). They who must not be identified—distinguishing personal from non-personal data under the GDPR. *International Data Privacy Law*, *10*(1), 35.

[466] Purtova, N. (2020). Organising concepts in law: A typology and lessons for data protection. *NFO-LEG [working paper],* 15.

[467] Van Lieshout, M. (2016). Privacy and Innovation: From Disruption to Opportunities. *Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection*, 195-212.

[468] Dalla Corte, L. (2020). Safeguarding Data Protection in an Open Data World: On the idea of balancing open data and data protection in the development, 14.

[469] Van der Sloot, B., & van Schendel, S. (2021). Procedural law for the data-driven society. *Information & Communications Technology Law*, *30*(3), 306.

[470] Koops, B. J. (2014). The trouble with European data protection law. *International data privacy law*, *4*(4), 250-261.

[471] Which was the focus of the former DPD and now of the GDPR, *see* Terstegge, J. (2020, February 4), Do we need a new GDPR? *NetKwesties*. Retrieved from https://www.netkwesties.nl/1421/do-we-need-a-new-gdpr.htm

causes, permitting structural issues to persist.[472] The static stages of data processing enshrined in the GDPR are inadequate for managing the dynamic nature of data in smart environments, where the *ex ante* data processing is often unclear.[473] The determination of the status of data is becoming increasingly challenging, which renders the notion that the boundary between personal and non-personal data is predetermined a fallacy.[474] Hence, without knowing how the data will be used, it is not clear what protections are appropriate.[475] An alternative approach would be to maintain the current differentiation between personal and non-personal data while implementing a more stringent framework for the latter.[476] This new approach recognizes the dynamic and contextual character of personal data.[477] To address these issues, the focus of the discussion on the material scope of data protection law should shift from the static concept of personal data to the processing of personal data.[478] The concept of personal data is intrinsically relational and necessitates a dynamic assessment within its particular processing instance to achieve enhanced comprehension.[479] It is imperative to note that personal data protection law applies to the processing of personal data, not personal data per se.[480] Upon considering, the expansive effects resulting from the combination of the low identifiability threshold and the broad range of ways in which information can be related to a natural person, as established by EU data protection law and jurisprudence, appear much less significant when personal data related to the data subject by virtue of its purpose or result within its lifecycle is considered, rather than statically.[481]

[472] Van der Sloot, B., & van Schendel, S. (2021). Procedural law for the data-driven society. *Information & Communications Technology Law*, *30*(3), 305.

[473] As argued by Axel Voss, rapporteur on the General Data Protection Regulation. *See* Espinoza, J (2021, March 4). EU data protection laws need overhaul, says policy architect; GDPR. *Financial Times (London, England).* Retrieved from https://advance-lexis-com.vu-nl.idm.oclc.org/api/document?collection=news&id=urn:contentItem:624G-V5C1-DYTY-C3DR-00000-00&context=1516831

[474] Purtova, N. (2018). The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, 10(1), 42-45.

[475] *See also* as discussed by Bert-Jaap Koops: "the assumption that data protection law should be comprehensive [...] stretches data protection to the point of breaking and makes it meaningless law in the books", Koops, B. J. (2014). The trouble with European data protection law. *International data privacy law*, *4*(4), 250-261.

[476] Van der Sloot, B., Van Schendel, S., & López, C. A. F. (2022). The influence of (technical) developments on the concept of personal data in relation to the GDPR. *TILT – Tilburg Institute of Law, Technology, and Society*, 10.

[477] Koops, B. J. (2014). The trouble with European data protection law. *International data privacy law*, *4*(4), 250-261.

[478] Van Der Sloot, B. (2017). *Privacy as virtue* (pp. 78). Intersentia.

[479] Dalla Corte, L. (2020). Safeguarding Data Protection in an Open Data World: On the idea of balancing open data and data protection in the development, 244.

[480] Gellert, R. M. (2021). Personal data's ever-expanding scope in smart environments and possible path (s) for regulating emerging digital technologies. *International Data Privacy Law*, 11(2), 207.

[481] Dalla Corte, L. (2019). Scoping personal data: towards a nuanced interpretation of the material scope of EU data protection law. *European Journal of Law and Technology*, *10*(1).

Additionally, it is noteworthy that smart cities are a socio-technical construct, whereas the GDPR adopts a technology and industry-neutral stance.[482] In theory, the technologically-neutral approach aims to ensure that legal protection remains effective despite the emergence of new technologies.[483] However, in practice, the dynamic nature of data protection may hinder the ability to draw definitive conclusions.[484] Smart city applications and their associated data technologies are inherently non-neutral due to potential influences from political and administrative processes, which may result in values that contradict legal principles.[485] The data-driven nature of smart cities highlights that nearly all data can be traced back to a person, rendering technology far from neutral.[486] The GDPR prioritises contextual integrity but remains both under- and over-inclusive in its definition of personal data, which is framed in an individualistic perspective and dependent on context.[487] The societal shift towards a data-driven paradigm has brought about a transformation in the nature of data processing. As a result, there has been a shift from analysing individual data to analysing statistical and aggregated data, from direct to derived data, and from certain to probabilistic information.[488] The aforementioned advancements have a profound impact on the existing structure of data protection regulations, specifically on the categorical approach. As a result, legal ambiguity arises due to the absence of

[482] Even though the technological aspect is a dominant element of the smart city narrative, the concept of smart city does not indicate any single technology or bundle of technologies. *See* Lazaro, C., & Metayer, D. L. (2015). Control over personal data: True remedy or fairy tale. *SCRIPTed*, *12*, 3.

[483] Hildebrandt, M., & Tielemans, L. (2013). Data protection by design and technology neutral law. *Computer Law & Security Review*, *29*(5), 509-521. It has been argued that "if it is neutral, it is not technology, *see* Strate, L. (2012). If it's neutral, it's not technology. *Educational Technology*, 6-9.

[484] Hildebrandt, M., & Tielemans, L. (2013). Data protection by design and technology neutral law. *Computer Law & Security Review*, *29*(5), 509-521.

[485] Hildebrandt, M., & Tielemans, L. (2013). Data protection by design and technology neutral law. *Computer Law & Security Review*, *29*(5), 509-521.

[486] Hildebrandt, M., & Tielemans, L. (2013). Data protection by design and technology neutral law. *Computer Law & Security Review*, *29*(5), 509-521. It has been argued that "if it is neutral, it is not technology, *see* Strate, L. (2012). If it's neutral, it's not technology. *Educational Technology*, 6-9.

[487] There are debates within the academic circle regarding the definition of personal data and the limitations of anonymization in protecting privacy. The current data protection laws only offer protection to individuals who are identifiable, but the advancements in data processing technologies have moved beyond the individualistic focus to a wider scope of analysis, such as the crowd. In this age of big data, data analytics technologies focus on groups of technology users and make inferences based on their lives and behaviours. As a result, privacy violations occur at the group level rather than at the individual level. This has raised concerns about the need for a new focus on group privacy, and the limitations of current data protection laws in addressing these privacy violations. It is suggested that the current emphasis on protecting personally identifying information should be supplemented by a focus on identifying information about categories or groups. The author of this thesis has limited the scope of their argument to exclude the topic of group privacy and due to the scope of this thesis the argument of group privacy will no longer be elaborated on. *See* Taylor, L., Floridi, L., & Van Der Sloot, B. (Eds.). (2016). *Group privacy: New challenges of data technologies* (Vol. 126) (pp. 5). Springer. On group privacy, *also see* Van Der Sloot, B. (2017). Do groups have a right to protect their group interest in privacy and should they? Peeling the onion of rights and interests protected under article 8 ECHR. *Group privacy: new challenges of data technologies*, 197-224.

[488] Bass, T., Sutherland, E., and Symons, T. (2018). Reclaiming the Smart City: Personal Data, Trust and the New Commons. Retrieved from https://media.nesta.org.uk/documents/DECODE-2018_report-smart-cities.pdf

guidelines regarding the establishment of contextual informational norms within a societal context.[489] To establish a technologically neutral framework, it may be imperative to enact technology-specific legislation and engage in in-depth deliberations regarding the legitimacy of activities in smart environments.[490]In some cases, technology-specific legislation and detailed provisions may be necessary to guarantee the neutrality of the law in regards to emerging technologies.[491]

Given the precedent, to facilitate practical and effective implementation of the law and avoid complex and individualised decisions, the GDPR should employ clear and specific language that minimises the scope for broad interpretations.[492] Sufficient detail is crucial for the GDPR to effectively mitigate the risks posed by inaccurate inferences, particularly in light of varying interpretations of its provisions among EU member states.[493] Successful implementation of such legislation requires expertise in both technology and law.[494] The increasing flow of data in smart cities necessitates a new approach to data protection that accounts for the dynamic and contextual nature of personal data. Ultimately, the goal is to achieve a framework that can adapt to new technological developments and preserve data protection in smart city environments.

6.2.1. Ensuring Effective Data Governance in Smart Environments

As technology advances at an unprecedented pace, it is imperative for the law to evolve alongside it to avoid becoming outdated or even inconsequential.[495] The conventional approach to data protection, which delineates between the public and private domains of information systems, has become obsolete in the current smart environment, where data is frequently exchanged across multiple domains and systems.[496] Furthermore, smart environments are characterised by their fluidity, constantly changing

[489] Hildebrandt, M., & Tielemans, L. (2013). Data protection by design and technology neutral law. *Computer Law & Security Review*, *29*(5), 509-521.

[490] Hildebrandt, M., & Tielemans, L. (2013). Data protection by design and technology neutral law. *Computer Law & Security Review*, *29*(5), 509-521.

[491] Hildebrandt, M., & Tielemans, L. (2013). Data protection by design and technology neutral law. *Computer Law & Security Review*, *29*(5), 509-521. It has been argued that "if it is neutral, it is not technology, *see* Strate, L. (2012). If it's neutral, it's not technology. *Educational Technology*, 6-9.

[492] Kröger, J. L. (2022). *Rogue Apps, Hidden Web Tracking and Ubiquitous Sensors* [Doctoral dissertation, Universität Berlin], 227–229.

[493] Fischer, C. (2020). The legal protection against inferences drawn by AI under the GDPR [L.L.M. thesis]. *Tilburg Law School, LL.M. Law and Technology.*

[494] Hildebrandt, M., & Tielemans, L. (2013). Data protection by design and technology neutral law. *Computer Law & Security Review*, *29*(5), 509-521. It has been argued that "if it is neutral, it is not technology, *see* Strate, L. (2012). If it's neutral, it's not technology. *Educational Technology*, 6-9.

[495] Stefanouli, M., & Economou, C. (2019). Data protection in smart cities: Application of the eu gdpr. In *Data Analytics: Paving the Way to Sustainable Urban Mobility: Proceedings of 4th Conference on Sustainable Urban Mobility (CSUM2018), 24-25 May, Skiathos Island, Greece* (pp. 748-755). Springer International Publishing.

[496] Kröger, J. L., Miceli, M., & Müller, F. (2021). How data can be used against people: a classification of personal data misuses [Preprint]. *Available at SSRN 3887097,* 10; Podda, E., & Palmirani, M. (2020). Inferring

according to the situation, and constantly evolving with the emergence of new technologies that may alter the categorization of data.[497] In smart cities, there are no clear boundaries between what constitutes personal and non-personal data.[498] The classification of data into legal categories is no longer an inherent characteristic of the data itself, but is rather dependent on the decisions and actions of the entities responsible for managing the data.[499] Thus, it is essential to carefully evaluate the context and purpose of data collection to determine how data should be classified and handled in order to guarantee the privacy and security of individuals.[500] Smart cities dissolve the boundaries between the public and private spheres, making the classification of data into 'personal' or 'non-personal' subjective and open to interpretation.[501] Evaluating the nature of data from a societal perspective requires a complex balancing of interests. Unlike the law, which remains static, everything in the environment is dynamic, and technology is constantly evolving, regardless of the current legal framework.[502] Whereas the law primarily focuses on categorising data as either personal or non-personal, technology processes the information without prejudice.[503] This shift in perception emphasises the importance of responsible data management and decision-making by controllers.[504] Prioritising and promoting privacy-by-design principles is essential, especially as the interrelation between law and technology seems to be absent in

the Meaning of Non-personal, Anonymized, and Anonymous Data. In *AI Approaches to the Complexity of Legal Systems XI-XII* (pp. 269-282). Springer, Cham.

[497] Hildebrandt, M. (2015). *Smart technologies and the end (s) of law: novel entanglements of law and technology*. Edward Elgar Publishing.

[498] Purtova, N. (2018). The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, *10*(1), 40-81.

[499] In a smart city environment, data is collected and managed by various entities, including local governments, private companies, and individuals. Thus, the classification of this data into legal categories is not solely determined by the nature of the data . This is due to the fact that the data collected and used in a smart city is often diverse and complex, and it is the responsibility of the data controllers to ensure that the data is processed and stored in compliance with relevant legal frameworks. Therefore, it is crucial for data controllers in smart cities to have a thorough understanding of the legal requirements and implications associated with the categorization of data, in order to ensure that the data is handled appropriately and lawfully. 'Controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data, Article 4 (7) GDPR.

[500] Hildebrandt, M. (2015). *Smart technologies and the end (s) of law: novel entanglements of law and technology*. Edward Elgar Publishing.

[501] Finck, M., & Pallas, F. (2020). They who must not be identified—distinguishing personal from non-personal data under the GDPR. *International Data Privacy Law*, *10*(1), 11-36.

[502] Choenni, S., Bargh, M. S., Busker, T., & Netten, N. (2022). Data governance in smart cities: Challenges and solution directions. *Journal of Smart Cities and Society*, 1-21.

[503] While in human intelligence, mental processes involve evaluative attributes like 'good' and 'bad', or 'right' and 'wrong', and include deductive assessments of theoretical nature, these are missing in smart city and its technological systems. Results generated by a smart city application are correlation-based and have an empirical status. They do not comply with the scientific concept of epistemics. *See* Solove, D. J. (2010). Fourth amendment pragmatism. *Boston College Law Review, 51*, 1528. *See also* Jastroch, N. (2020). Trusted artificial intelligence: on the use of private data. In *Product Lifecycle Management Enabling Smart X: 17th IFIP WG 5.1 International Conference, PLM 2020, Rapperswil, Switzerland, July 5–8, 2020, Revised Selected Papers 17* (pp. 659-670). Springer International Publishing.

[504] Christofi, A., Wauters, E., & Valcke, P. (2021). Smart Cities, Data Protection and the Public Interest Conundrum: What Legal Basis for Smart City Processing?. *European Journal of Law and Technology*, *12*(1), 1-36.

practical applications of personal data.[505] Despite the EU legislation calling for data protection by design and by default,[506] there is still a margin of uncertainty about its meaning and implementation [507] For instance, when developing a new software application that gathers personal data, legal requirements dictate that data protection must be considered during the design and development stages.[508] However, there is a dearth of explicit guidance concerning the specific measures that must be taken to achieve compliance and maintain data protection measures as the software evolves and new features are added.[509] This lack of clarity may result in divergent approaches to data protection implementation across different organisations, potentially jeopardising the security and integrity of individuals' personal data.[510] A paucity of robust design mandates can compromise the efficacy of the GDPR.

To tackle these challenges, it is necessary to move beyond protecting personal information from public disclosure and shift towards smart governance.[511] In a data-driven society, the development and maintenance of dependable data management frameworks is of utmost importance.[512] A suggestion in this sense is to start focusing on the practical issue of how best to regulate information gathering and use in smart cities.[513] Accordingly, it is suggested to incorporate information security and to govern the

[505] European Data Protection Supervisor (2018). Opinion 5/2018–Preliminary Opinion on Privacy by Design. Retrieved from https://edps.europa.eu/

[506] Art. 25 GDPR, Data protection by design and by default

[507] Jasmontaite, L., Kamara, I., Zanfir Fortuna, G., & Leucci, S. (2018). Data protection by design and by default: Framing guiding principles into legal obligations in the GDPR. *European Data Protection Law Review*, *4*(2), 168-189.

[508] Jasmontaite, L., Kamara, I., Zanfir Fortuna, G., & Leucci, S. (2018). Data protection by design and by default: Framing guiding principles into legal obligations in the GDPR. *European Data Protection Law Review*, *4*(2), 168-189; Waldman, A. E. (2020). Data Protection by Design? A Critique of Article 25 of the GDPR. *Cornell International Law Journal, 53*, 147.

[509] Waldman, A. E. (2020). Data Protection by Design? A Critique of Article 25 of the GDPR. *Cornell International Law Journal, 53*, 147.

[510] Therefore, clear guidelines and best practices for data protection by design and by default must continue to be developed to ensure proper safeguarding of personal data. Moreover, the implementation of data protection by design and by default in the EU should not only target software developers or hardware producers, but also controllers. Only by including all parties involved in data processing can data subjects receive comprehensive and meaningful protection of their personal data. *See* Jasmontaite, L., Kamara, I., Zanfir Fortuna, G., & Leucci, S. (2018). Data protection by design and by default: Framing guiding principles into legal obligations in the GDPR. *European Data Protection Law Review*, *4*(2), 168-189.

[511] Due to the limited scope of this thesis, I will not further go into particularities of security governance and information security. However, it is worthwhile to highlight the dependencies between data protection and cybersecurity and the fact that privacy protection requires establishing cybersecurity. Information sharing is one of the pillars of cybersecurity, especially in distributed settings such as the smart city. *See* Dalla Corte, L. (2020). Safeguarding Data Protection in an Open Data World: On the idea of balancing open data and data protection in the development, 14.

[512] Van der Sloot, B., & Keymolen, E. (2022). Can we trust trust-based data governance models?. *Data & Policy*, *4*, 45.

[513] Smart Governance is defined as "the capacity of employing intelligent and adaptive acts and activities of looking after and making decisions about something", Scholl, H. J., & AlAwadhi, S. (2016). Creating Smart Governance: The key to radical ICT overhaul at the City of Munich. *Information Polity*, *21*(1), 22. *Also see* Pereira, G. V., Parycek, P., Falco, E., & Kleinhans, R. (2018). Smart governance in the context of smart cities: A literature review. Information Polity, 23(2), 143-162.

use of data and the actual application of data.[514] Surprisingly, the term 'data governance' does not appear in the official text of GDPR, but it is at the core of what the regulation stands for.[515] The governance of a data ecosystem within smart cities requires that the collection and processing of personal data is limited to what is necessary and proportional.[516] To achieve proper smart governance, it is important to adopt a comprehensive approach that balances the benefits of data collection and processing with the privacy rights of individuals.[517] The first step in achieving this balance is to limit the collection and processing of personal data to what is strictly necessary and proportional.[518] Effective data governance requires a careful balancing of the interests of stakeholders and a continual reassessment of the risks and benefits associated with personal data in the smart city ecosystem.[519] The GDPR provides the framework for this shift by emphasising the need of data protection principles in the whole data ecosystem of the city, such as accountability, purpose limitation, data minimization, and data protection

[514] Data governance is found on the following guiding principles: integrity, transparency, auditability, accountability, stewardship, standardisation and change management. The proposed Data Governance Act would be the first piece of legislation to underpin the European data strategy. This new approach to data sharing outlined by the European Commission could accelerate smart city initiatives. *See* European Commision (2020), COM(2020) 767 final, 2020/0340(COD) *Data Governance Act. Also see* Johnson, J., Hevia, A., Yergin, R., Karbassi, S., Levine, A., & Ortiz, J. (2022). Data governance frameworks for smart cities: key considerations for data management and use. *Journal of Law and Mobility*, *2022*(1), 1; European Union Agency for Network and Information Security (ENISA) (2017). Handbook on Security of Personal Data Processing. *ENISA*.

[515] Voss, W. G. (2019). Cross-border data flows, the GDPR, and data governance. *Washington International Law Journal*, *29*, 485.

[516] This is reflected in the principle of "data minimization" laid down in Art. 6 (1) lit.c GDPR. *See* Franke, J., & Gailhofer, P. (2021). Data governance and regulation for sustainable smart cities. *Frontiers in Sustainable Cities*, *3*, 148.

[517] While the GDPR should precede the DGA, a mutual coordination of these acts is found to be useful as they can interact in the field of data governance. The DGA recognises the legitimate objectives to foster the availability of data through the establishment of data intermediary structures and strengthening data sharing mechanisms across the EU, and thus can be a starting point for proper data governance within European data protection law. As stated in the Explanatory memorandum to the DGA proposal: "(...) the interplay with the legislation on personal data is particularly important. With theGeneral Data Protection Regulation (GDPR) and e-Privacy Directive, the EU has put in place a solid and trusted legal framework for the protection of personal data and a standard for the world". *See* Vardanyan, L., & Kocharyan, H. The GDPR and the DGA Proposal: are They in Controversial Relationship?. *European Studies*, *9*(1), 91-109.
Choenni, S., Bargh, M. S., Busker, T., & Netten, N. (2022). Data governance in smart cities: Challenges and solution directions. *Journal of Smart Cities and Society*, 1-21.

[518] This is already established under the GDPR, article 5(1)(c) GDPR. Notably, to realise data governance within a data domain, several measures should be taken. Data governance realisation may call for introducing some (new) roles within a data ecosystem such as data steward and (chief) data officer roles. Often, these mechanisms are complex and therefore a successful deployment of smart cities asks for disseminating data governance knowledge among the involved parties so that they (i.e. citizens and organisations) who reside closely to their data can play their roles in maintaining the quality of their data as well as protecting their data, *see* Choenni, S., Bargh, M. S., Busker, T., & Netten, N. (2022). Data governance in smart cities: Challenges and solution directions. *Journal of Smart Cities and Society*, 1-21.

[519] Nevertheless, there is still a lack of research that uncovers whether online forms of collaboration and (smart) governance truly result in offline improvements in the quality of life. Paragraph 6.1.1. on the realistic risk approach to personal data. *See* Choenni, S., Bargh, M. S., Busker, T., & Netten, N. (2022). Data governance in smart cities: Challenges and solution directions. *Journal of Smart Cities and Society*, 1-21.

by design and default.[520] Ultimately, effective data governance will require a combination of legal, technical, and social solutions to ensure that personal data is collected, stored, and used in a responsible and ethical manner.[521] To address these challenges, there is a growing need for more robust and comprehensive data governance frameworks.[522] This will involve investment in data management and security infrastructure, the development of technical tools and best practices for data protection, as well as education and awareness campaigns for both data controllers and data subjects.[523] The practical implementation of these principles in a rapidly evolving technological landscape requires innovative and forward-looking solutions.[524]

6.2.2. The Dynamic Life Cycle of Data and Smart Cities: Rethinking Personal Data Protection

The permeation of data-driven technologies in smart cities is on the rise, and this highlights the need for data protection laws to consider the dynamic life cycle of data.[525] It has been argued that using clearly defined and delimited categories of data is only effective if the data remains consistently categorised. However, this is increasingly less likely due to the volatile nature of data.[526] An initially innocuous dataset containing ordinary personal data can quickly become sensitive data when linked and

[520] This is reflected in the principle of "data minimization" laid down in Article 5(1)(c) GDPR. *See* Franke, J., & Gailhofer, P. (2021). Data governance and regulation for sustainable smart cities. *Frontiers in Sustainable Cities*, *3*, 148.

[521] Choenni, S., Bargh, M. S., Busker, T., & Netten, N. (2022). Data governance in smart cities: Challenges and solution directions. *Journal of Smart Cities and Society*, 1-21.

[522] Franke, J., & Gailhofer, P. (2021). Data governance and regulation for sustainable smart cities. *Frontiers in Sustainable Cities*, *3*, 148.

[523] Choenni, S., Bargh, M. S., Busker, T., & Netten, N. (2022). Data governance in smart cities: Challenges and solution directions. *Journal of Smart Cities and Society*, 1-21; Dalla Corte, L. (2020). Safeguarding Data Protection in an Open Data World: On the idea of balancing open data and data protection in the development, 10.

[524] Nonetheless, data governance remains a complex and evolving field. Many organisations continue to struggle with the implementation of effective data governance practices, particularly in light of the rapidly evolving landscape of data-driven technologies. Effective data governance requires collaboration and coordination between these stakeholders, including data controllers, data processors, data subjects, and regulators. *See* Dalla Corte, L. (2020). Safeguarding Data Protection in an Open Data World: On the idea of balancing open data and data protection in the development, 10; Denker, A. (2021). Protection of Privacy and Personal Data in the Big Data Environment of Smart Cities. *The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences*, *XLVI-4/W5*-2021, 181-186.

[525] Podda, E., & Palmirani, M. (2020). Inferring the Meaning of Non-personal, Anonymized, and Anonymous Data. In *AI Approaches to the Complexity of Legal Systems XI-XII* (pp. 269-282). Springer, Cham. p. 271

[526] Van der Sloot, B., Van Schendel, S., & López, C. A. F. (2022). The influence of (technical) developments on the concept of personal data in relation to the GDPR. *TILT – Tilburg Institute of Law, Technology, and Society*, 17.

enriched with another dataset.[527] Considering the ease with which a dataset can be quickly reclassified, it is worth questioning the practicality of utilising clearly defined categories.[528] The definition of personal data is constantly evolving, which can rapidly transform non-personal data into personal data, posing challenges for effectively managing data in smart cities.[529] It is essential to recognize that the smart city is not just a collection of its applications. Furthermore, although individual smart city applications may not always appear to violate data protection rights, the combination of these applications can result in increased risks.[530] To address this issue, the GDPR must be updated to account for the dynamic nature of data in smart city environments.[531] Instead of making a blanket statement that inferences are considered personal data, it would be more appropriate to acknowledge that the definition allows for inferences to be treated as personal data in some cases.[532]

To simplify the legal framework for determining the legitimacy of data processing, a unified test for all stages of personal data's life cycle is needed.[533] This requires a flexible and adaptive approach to interpreting personal data, taking into account how data is collected and processed over time.[534] Instead of a static definition, personal data should be defined based on its purpose or result within the data lifecycle.[535] By focusing on the most stable period of time that data is considered personal, it is possible to provide greater clarity and consistency in defining personal data, while also accommodating the changing nature of data over time.[536] In addition to identifying the most stable period of time, it is also important to identify vulnerability points in the data lifecycle to better protect personal data where

[527] Van der Sloot, B., Van Schendel, S., & López, C. A. F. (2022). The influence of (technical) developments on the concept of personal data in relation to the GDPR. *TILT – Tilburg Institute of Law, Technology, and Society*, 17.

[528] The resulting data may then be aggregated or stripped of identifiers, and subsequently de-anonymized or integrated into yet another dataset to create personal data. These transformations can occur within a matter of seconds. *See* Van der Sloot, B., Van Schendel, S., & López, C. A. F. (2022). The influence of (technical) developments on the concept of personal data in relation to the GDPR. *TILT – Tilburg Institute of Law, Technology, and Society*, 17.

[529] Gellert, R. (2021). Personal data's ever-expanding scope in smart environments and possible path(s) for regulating emerging digital technologies. *International Data Privacy Law,* 11(2), 206.

[530] Ammara, U., Rasheed, K., Mansoor, A., Al-Fuqaha, A., & Qadir, J. (2022). Smart cities from the perspective of systems. *Systems*, *10*(3), 77.

[531] Data that is not initially related to a data subject based on its content but rather its purpose or outcome may still end up being related to the data subject throughout its entire life cycle, depending on the type of data and how it is processed, but this is only a potential scenario. On the other hand, data that does relate to a data subject based on its content will remain related to the data subject throughout its entire life cycle, regardless of how it is processed.

[532] Fischer, C. (2020). The legal protection against inferences drawn by AI under the GDPR [L.L.M. thesis]. *Tilburg Law School, LL.M. Law and Technology.*

[533] Moerel, L., & Prins, C. (2016). Privacy for the homo digitalis: Proposal for a new regulatory framework for data protection in the light of Big Data and the internet of things, 12.

[534] Podda, E., & Palmirani, M. (2020). Inferring the Meaning of Non-personal, Anonymized, and Anonymous Data. In *AI Approaches to the Complexity of Legal Systems XI-XII* (pp. 269-282). Springer, Cham. p. 271

[535] Dalla Corte, L. (2020). Safeguarding Data Protection in an Open Data World: On the idea of balancing open data and data protection in the development, 234.

[536] Dalla Corte, L. (2020). Safeguarding Data Protection in an Open Data World: On the idea of balancing open data and data protection in the development, 234.

it is most vulnerable.[537] This involves understanding the various phases of the data lifecycle, from collection to processing to destruction, and identifying potential risks to personal data at each stage.[538] By doing so, appropriate measures can be put in place to protect personal data, and ensure that it is handled in a responsible and secure manner.[539]

Ensuring successful personal data protection in smart cities requires embedding data protection requirements within the entire lifecycle of smart city technologies.[540] This includes considering the management of existing and new information systems, as well as the secondary uses that may arise over time, such as function creep.[541] It is important for the definition of personal data to take into account the context in which data is collected and processed, as individuals in a smart city environment may generate personal data simply through their presence, even if they were not the intended targets.[542] All things considered, the dynamic life cycle of data in smart cities highlights the importance of considering both the technical innovative character of smart cities and the protection of individuals' right to protection of their personal data.[543] The new interpretation of the concept of personal data must balance these two goals in a comprehensive manner. The GDPR should be able to respond to (technological) change not only by being technologically neutral (ie. not discriminating against particular technologies),[544] but also incorporating flexible and adaptive measures that allow for updates in response to emerging technologies. Nonetheless, effectively addressing the technological character of smart cities from a legal perspective remains a challenge.

[537] This model of life cycle describes the traditional processing of personal data by a sequence of phases beginning from giving of personal data by individual and finishing with personal data destroying (by the data controller) after the goal realisation. Such a baseline measurement establishes the situation of the flow of an information system's data throughout its lifecycle.

[538] Moerel, L., & Prins, C. (2016). Privacy for the homo digitalis: Proposal for a new regulatory framework for data protection in the light of Big Data and the internet of things, 12.

[539] Galdon-Clavell, G. (2013). (Not so) smart cities?: The drivers, impact and risks of surveillance-enabled smart environments. *Science and Public Policy*, *40*(6), 717-723.

[540] Denker, A. (2021). Protection of Privacy and Personal Data in the Big Data Environment of Smart Cities.The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences, *XLVI-4/W5-202*1, 181-186.

[541] Choenni, S., Bargh, M. S., Busker, T., & Netten, N. (2022). Data governance in smart cities: Challenges and solution directions. *Journal of Smart Cities and Society*, 1-21.

[542] Gellert, R. M. (2021). Personal data's ever-expanding scope in smart environments and possible path (s) for regulating emerging digital technologies, *International Data Privacy Law, 2021, 11*(2)*,* 202.

[543] Purtova, N. (2020). Code as personal data. *INFO-LEG* [working paper], 10.

[544] Recital 15 GDPR

6.3. Conclusion.

The GDPR is characterised by a highly contextual core, yet it also contains elements of a categorical approach.[545] In this regard, there exists a marked ambivalence within EU data protection law with respect to the concept of personal data. [546] The contextual definition of personal data, which takes into account the specific circumstances of a case, is advantageous in that it allows for the consideration of all relevant aspects and can adapt to changing circumstances, thereby avoiding obsolescence or circumvention. However, this fluid and contextual regulatory approach also suffers from a lack of legal certainty, both for data controllers and data subjects.[547] Conversely, the categorical approach provides fixed definitions and clear regulatory rules, which offer greater legal certainty. Nonetheless, this approach is vulnerable to circumvention, obsolescence, and lacks the granularity of the contextual approach.[548] While a precise equilibrium appears to be absent, it is nonetheless necessary.

In contemporary times, technology operates in a neutral manner and does not differentiate between information that is deemed favourable or unfavourable, nor does it classify data as personal or non-personal. Rather, it is the data protection regulations that make such distinctions. In the era of smart cities, reconciling legal and technical standards to ensure the safeguarding of personal data poses a considerable challenge. The concept of personal data already presents challenges due to its individual requirements of identifiability and relating to, but these issues become even more complex when these elements interact. As a result, the interpretation of the concept of personal data can impede the effective functioning of data protection laws in smart cities. The outdated text and interpretations of the GDPR can hinder innovation and the proper functioning of smart cities.[549] In order to effectively manage data protection rights in a smart city environment, there should be greater emphasis on the use and reuse of

[545] Upon initial examination, the data protection regime appears to be primarily characterised by a categorical approach that lacks the contextual or harm-based element that is integral to human rights evaluations. This binary approach is evident throughout the framework. However, there is also evidence of a contextual approach in some aspects of the regime. For example, while the distinction between personal and non-personal data is binary, the definition of personal data incorporates contextual factors. As a result, the obligations and requirements imposed by the data protection regime are largely dependent on the particular circumstances of the case. In general, as the amount and sensitivity of data collected increases, and as the risk associated with data processing or the number of parties involved in the process increases, the rules and obligations become more stringent. Nonetheless, there are certain context-dependent limitations to the obligations and requirements set forth in the GDPR.

[546] Van der Sloot, B., Van Schendel, S., & López, C. A. F. (2022). The influence of (technical) developments on the concept of personal data in relation to the GDPR. *TILT – Tilburg Institute of Law, Technology, and Society*, 10.

[547] Van der Sloot, B., Van Schendel, S., & López, C. A. F. (2022). The influence of (technical) developments on the concept of personal data in relation to the GDPR. *TILT – Tilburg Institute of Law, Technology, and Society*, 10.

[548] Van der Sloot, B., Van Schendel, S., & López, C. A. F. (2022). The influence of (technical) developments on the concept of personal data in relation to the GDPR. *TILT – Tilburg Institute of Law, Technology, and Society*, 10.

[549] *See* Hildebrandt, M., & Tielemans, L. (2013). Data protection by design and technology neutral law. *Computer Law & Security Review*, *29*(5), 509-521.

data, with a focus on balancing proper functioning of the city with the protection of personal data. To ensure legal enforceability in the face of advancing technologies and evolving social contexts, it is essential that definitions remain flexible and innovative.[550] The current legislation may not be adequate to cope with the changing scope of personal data and its associated risks posed by smart technologies, making it imperative for the legislator to adjust the provisions of the GDPR to reflect the current and future technical realities. Data governance is essential for appropriate use of data in smart cities, with a focus on balancing personal data protection and data quality, as the flow of data through these environments is complex and multidimensional. The starting point should always be that personal data is sacrosanct and must be protected. In this context, it is important to adjust the provisions of the GDPR to current and future technical advancements and realities. The establishment of an effective framework for the concept of personal data in smart cities should entail its comprehensive consideration of the extensive capabilities of modern technology, by incorporating the potential for harm and the realistic risk of identification.

A flexible concept of personal data, which considers personal data as a continuous determinant rather than a binary concept, can help to resolve the trade-off between data protection and data quality in smart cities. However, some challenges require wider societal and political debates. This includes exploring the relationship between personal data and statistical disclosure in smart cities, and how the law, (personal) data, and technologies interact and affect these environments. Adjusting the requirements or adopting a new concept of personal data is necessary for a sustainable future of data protection. This is a complex matter that requires collaboration between multiple perspectives from both the legal and technical realms. The law should not be static merely preserving the status quo but should be adapted to reflect the changing needs of society and the environment. Through a process of iteration and dynamic steering, this will be an ongoing work in progress.

[550] Denker, A. (2021). Protection of Privacy and Personal Data in the Big Data Environment of Smart Cities.The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences, XLVI-4/W5-2021, 181-186.

Chapter VII.

Conclusion

The ubiquity of digital technologies has made data the cornerstone of the functioning of the globalised world, giving rise to the emergence of smart cities, where data-driven technologies are interwoven into the fabric of urban life. As society progressively transitions to a data-centric future, the legitimacy and efficacy of data protection laws have come under scrutiny. In this new 'datafied' state, where virtually all activities are monitored through technologies, the smart environment highlights the importance of reliable data management structures that adhere to legal requirements and respect digital privacy. The broad and flexible nature of the definition of personal data in Article 4(1) of the GDPR has been criticised for its loopholes that impede its efficacy. Smart cities introduce additional complexities and unique challenges that further complicate the definition of personal data. This thesis analyses the regulatory purpose of the GDPR, yielding valuable insights into the risks associated with both under- and over-regulation, as well as the regulatory gaps that arise owing to the disparity between the legal and technological realms. Moreover, the thesis has explored potential alternatives to the current concept of personal data. The research conducted in this thesis aimed to examine the legal challenges arising from the current interpretation and application of personal data under Article 4(1) of the GDPR in light of the smart city of the future, in order to address the main research question:

"To what extent is the current interpretation and application of 'personal data', as envisaged in Article 4(1) of the GDPR, suitable and sustainable in light of the permeation of data-driven technologies, such as the smart city?"

In this concluding chapter, the answer to the research questions will be provided, encompassing all that has been discussed thus far. The first sub-question explored the material scope of the GDPR by examining "*What is the current interpretation of personal data as envisaged in Article 4(1) of the GDPR by European case law and bodies, and how has this interpretation evolved over time?"* and is addressed in Chapter 2. Personal data constitutes a fundamental pillar of the GDPR and is built on the premise of its conceptualization, defined as information relating to an identified or identifiable natural person. In response to technological developments, the legal definition of personal data has expanded the notion of personal data over time to include both direct and indirect information, as well as information that may lead to identification in the future. To ascertain whether a dataset contains identifiable information, all legal reasonably means likely to be used to identify the data subject must be considered. The wide interpretation has been further broadened by the Article 29 Working Party and by the Court of Justice of the European Union by emphasising the requirements of 'identifiability' and 'relating to'. However, as technology continues to advance and open data initiatives such as smart cities gain momentum, determining what qualifies as personal data has become progressively complicated. The expanding nature of personal data has resulted in a larger number of datasets falling under the purview of the data protection regime. The broad and flexible nature of the concept, along with its low threshold for identifiability, has blurred the line between personal and non-personal data, leading to an ambiguous definition of personal data. Furthermore, the contextual nature of the definition further complicates this distinction, as it is relative and open to interpretation, affecting the GDPR's effectiveness in protecting data subjects. The categorization of data under legal categories is no longer an inherent feature of the data itself, but rather determined by the decisions and actions of those responsible for managing the data. Therefore, a clear and consistent definition of personal data is crucial for its legal interpretation and the protection of data subjects in the evolving technological landscape.

Subsequently, chapters three, four, and five provide an answer to the second sub-question, "*What are smart cities and what are the specific challenges to the concept of personal data as envisaged in Article 4(1) of the GDPR posed by smart cities for the protection of personal data rights?*". Smart cities are urban environments that leverage digital technologies to optimise various aspects of city life, generating vast amounts of data that are frequently analysed to extract insights and improve decision-making. However, the use of these technologies poses significant challenges in protecting personal data rights as a substantial amount of data falls under the classification of personal data as envisaged in the GDPR. The proliferation of data-driven technologies and persistent advocacy for open data and information repurposing in smart cities have created a more fluid legal status for data. As a result, the current definition of 'personal data' under Article 4(1) of the GDPR is more inclusive and encompasses a broader range of data-related aspects. Personal data is a fundamental operational resource for smart cities, making it even more crucial to ensure that the data is protected. The permeation of data-driven technologies, such as the future smart city, has made it progressively effortless to extract personal data from aggregated, anonymized, or encrypted datasets. Identification is becoming more effortless, and information can be linked to identifiable natural persons in multiple ways, such as through its content, purpose, or result. Moreover, the legal distinction between non-personal data and personal data is binary and absolute, however, the criteria for determining whether data is personal are contextual and subject to interpretation. The GDPR's arbitrary classifications and blurred lines make it difficult to provide adequate protection to personal data at a specific moment in time as the status of data is constantly evolving. The concept of personal data, based on the identifiability/anonymity dichotomy, can be viewed as overly expansive and unclear, posing challenges due to the GDPR's wide-ranging applicability. A corollary that is often overlooked is the intricate interdependence of technologies and their environment that contributes to the potentially boundless nature of the concept of personal data. In the context of smart cities, where datafication encompasses all aspects of the environment and individuals, the definition of personal data is becoming increasingly intricate. The semantic ambiguity of the definition of personal data highlights the necessity of enhanced lucidity and uniformity in its implementation throughout the European Union. Therefore, the thesis puts forth the hypothesis that the application of the concept of personal data in the context of smart cities is unrealistic and emphasises the need for greater clarity and consistency in its application.

Finally, chapter six addresses the third sub-question of the thesis "*How does the implementation of the concept of personal data as envisaged in Article 4(1) of the GDPR in smart cities impact the protection of personal data rights, and what can be done to ensure that this protection is maintained in the face of the increasing data processing in smart environments?*". The thesis contends that the application of the concept of personal data in smart cities has noteworthy implications that complicate safeguarding the protection of natural persons with regard to the processing of personal data, hindering proper implementation of the GDPR. This challenge arises from a disconnection between the legal framework and the technical reality, namely the GDPR and smart cities, as the former operates within a technology and industry-neutral framework, while the latter is based on socio-technical constructs. The thesis suggests that upfront regulation of specific processing activities may not be effective due to the contextual nature of data processing. Furthermore, relying solely on the nature of the data as an approach to personal data protection is not sufficiently robust and found to be insufficient. To address the aforementioned issues, the thesis suggests adopting a risk-based approach that centres on the potential risks and harms associated with data processing. In this regard, data protection regulations should be customised to suit the level of risk posed by various types of data, prioritising protection against actual harms as opposed to classification. Moreover, an interesting avenue to address the challenges posed by smart environments, is the implementation of smart data governance as a means of addressing the challenges posed by the dynamic life cycle of data in smart cities. Updating the definition of personal data under the GDPR to reflect smart environments will ensure sustainable protection in light of other data-driven technologies. Discussions should be initiated to determine the boundaries for data use. As smart cities challenge our comprehension of personal data, it is imperative to keep pace with the evolving technologies instead of attempting to restrict it. The establishment of a holistic approach to data management, with a focus on adaptability and flexibility to accommodate emerging technologies, is crucial for ensuring sustainable protection of personal data.

To answer the main research question, this thesis concludes that the existing application and interpretation of the concept of personal data is insufficient and unsustainable in protecting individuals' personal data, and this is compounded by the unpreceded availability of advanced technologies. The tension between data-driven technologies in the smart city and the current legal definition of personal data exacerbates the issue. Indeed, the complex and multifaceted nature of the smart city context demands meticulous attention to protect a person's information and ensure societal benefits from technological advancements. The primary concern does not solely revolve around balancing data processing and safeguarding personal data, because the issue of data protection is not just about striking a balance between two opposing factors. Rather, it pertains to demarcating the material ambit of legislation that governs data protection, as well as determining what constitutes personal data. The emergence of novel and unpredictable technologies poses a challenge for regulators, as the impact cannot be anticipated until after deployment. As a response to this challenge, the concept of personal data has expanded over time, and a sustainable and future-proof comprehension of personal data must encompass technical, legal, and societal aspects. The discourse on regulatory objectives in smart environments remains unresolved, as evaluating regulatory gaps and alternative solutions is challenging in light of ongoing discussions. The integration of data-driven technologies in smart cities is continuously evolving, which poses difficulties in developing regulatory frameworks that can keep up with technological advancements. To address the gaps effectively, it is essential to determine the most appropriate regulatory approach that can balance competing interests. However, there is no clear consensus on the optimal approach, with categorical, contextual, and hybrid regulatory approaches each having their advantages and disadvantages. Thus, it is imperative to ensure effective synergy between technological innovation and personal data protection to achieve effective development of smart cities where personal data is adequately protected. As this complex terrain is navigated, it is important to note that personal data is not merely a legal or technical concept but also an essential aspect of individual identity and autonomy. The broadening of the concept of personal data is a natural reaction to its application within smart cities, influenced by the dynamic world we live in. Ultimately, it is only through a holistic understanding and recognition of the multidimensional nature of personal data that a truly sustainable and responsible future for smart cities can be created.

Bibliography

PRIMARY SOURCES

Cases

Breyer, Case C-582/14, [2016] (ECLI:EU:C:2016:779)

Nowak, Case-434/16, [2017], (ECLI:EU:C:2017:994)

Volker und Markus Schecke GbR v Land Hessen, CJEU, Joined Cases no. C92/09 and C-93/09, [2010], ECR 2010 I-11063 (ECLI:EU:C:2010:662)

Bodil Lindqvist, Case C-101/01, [2003], (ECLI:EU:C:2003:596).

YS and MS v. Minister voor Immigratie, Integratie en Asiel, [2014], Joined Cases C-141/12 and C-372/12 (ECLI:EU:C:2014:208)

SECONDARY SOURCES

Alaverdyan, D., Kučera, F., & Horák, M. (2018). Implementation of the smart city concept in the eu: importance of cluster initiatives and best practice cases. *International Journal of Entrepreneurial Knowledge*, *6*(1).

Ambrose, M. L. (2012). It's about time: privacy, information life cycles, and the right to be forgotten. *Stanford Technology Law Review*, *16*, 369.

Ammara, U., Rasheed, K., Mansoor, A., Al-Fuqaha, A., & Qadir, J. (2022). Smart cities from the perspective of systems. *Systems*, *10*(3), 77.

Article 29 Working Party, Opinion 03/2013 on Purpose Limitation (‘WP 203’).

Article 29 Working Party, Opinion 04/2014 on Anonymisation Techniques (‘WP 216’).

Article 29 Working Party, Opinion 4/2007 on the Concept of Personal Data (‘WP136’).

Barocas, S., & Nissenbaum, H. (2014). Big data’s end run around anonymity and consent. *Privacy, big data, and the public good: Frameworks for engagement*, *1*, 44-75.

Bass, T., Sutherland, E., and Symons, T. (2018). Reclaiming the Smart City: Personal Data, Trust and the New Commons. Retrieved from https://media.nesta.org.uk/documents/DECODE-2018_report-smart-cities.pdf

Borgesius, F. J. Z. (2016). Singling out people without knowing their names–Behavioural targeting, pseudonymous data, and the new Data Protection Regulation. *Computer Law & Security Review*, *32*(2), 256-271.

Boscolo, P , Bourmpos, M., Datani, I, Garre, A. G., Keunen, V., Molina-Ríos, B., Palmisano, E., & Tsiligkiri, C. (2021). Case Studies Involving the Use of Personal Data in a Smart City. In S. Topham, P. Boscolo, & M. Mulquin (Eds.)*, Personal Data-Smart Cities: How cities can Utilise their Citizen's Personal Data to Help them Become Climate Neutral* (pp. 71-95). River Publishers.

Breuer, J., & Pierson, J. (2021). The right to the city and data protection for developing citizen-centric digital cities. *Information, Communication & Society*, *24*(6), 801.

Breuer, J., Van Zeeland, I., Pierson, J., & Heyman, R. (2019,). The Social Construction of Personal Data Protection in Smart Cities. In *2019 CTTE-FITCE: Smart Cities & Information and Communication Technology (CTTE-FITCE)* (pp. 1-6). IEEE.

Brown, T. E. (2019). Human Rights in the Smart City: Regulating Emerging Technologies in City Places. *Regulating New Technologies in Uncertain Times*, 47-65.

Chen, Z., Yan, L., Lü, Z., Zhang, Y., Guo, Y., Liu, W., & Xuan, J. (2021). Research on zero-trust security protection technology of power IoT based on blockchain. In *Journal of Physics: Conference Series* (Vol. 1769, No. 1, p. 012039). IOP Publishing.

Choenni, S., Bargh, M. S., Busker, T., & Netten, N. (2022). Data governance in smart cities: Challenges and solution directions. *Journal of Smart Cities and Society*, 1-21.

Christofi, A. (2021). Smart cities and the data protection framework in context. *SPECTR.*

Christofi, A., Wauters, E., & Valcke, P. (2021). Smart Cities, Data Protection and the Public Interest Conundrum: What Legal Basis for Smart City Processing?. *European Journal of Law and Technology*, *12*(1), 1-36.

Coetzee, S., Ivánová, I., Mitasova, H., & Brovelli, M. A. (2020). Open geospatial software and data: A review of the current state and a perspective into the future. *ISPRS International Journal of Geo-Information*, *9*(2), 90.

Council of Europe (2010), The Protection of Individuals with Regard to Automatic Processing of Personal Data in the Context with Regard to Automatic Processing. *Recommendation CM/Rec(2010)13 and Explanatory Memorandum.*

Creţu, A. M., Monti, F., Marrone, S., Dong, X., Bronstein, M., & de Montjoye, Y. A. (2022). Interaction data are identifiable even across long periods of time. *Nature communications*, *13*(1), 1-11.

Dalla Corte, L. (2019). Scoping personal data: towards a nuanced interpretation of the material scope of EU data protection law. *European Journal of Law and Technology*, *10*(1).

Dalla Corte, L. (2020). Safeguarding Data Protection in an Open Data World: On the idea of balancing open data and data protection in the development, 1-14.

Dalla Corte, L. (2022). Personal Data in the EU Legal System. In *Elgar Encyclopaedia of Law and Data Science* (pp. 259-267). Edward Elgar.

Dalla Corte, L., van Loenen, B., & Cuijpers, C. (2017). Personal Data Protection as a Nonfunctional Requirement in the Smart City's Development. In B. Anglès Juanpere, & J. Balcells Padullés (Eds.), *Proceedings of the 13th International Conference on Internet, Law & Politics: Managing Risk In the Digital Society* (pp. 76-92). Huygens Editoria.

Daoudagh, S., Marchetti, E., Savarino, V., Bernabe, J. B., García-Rodríguez, J., Moreno, R. T., ... & Skarmeta, A. F. (2021). Data Protection by Design in the Context of Smart Cities: A Consent and Access Control Proposal. *Sensors*, *21*(21), 7154.

De Conca, S. (2021). *The enchanted house: An analysis of the interaction of intelligent personal home assistants (IPHAs) with the private sphere and its legal protection.*

De Hert, P. (2017). Data protection's future without democratic bright line rules: Co-existing with technologies in Europe after Breyer. *European Data Protection Law Review,* 3(1), 27-30.

Denker, A. (2021). Protection of Privacy and Personal Data in the Big Data Environment of Smart Cities.*The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences, XLVI-4/W5-2021*, 181-186.

Ducuing, C. (2021). The regulation of 'data': a new trend in the legislation of the European Union? *KU Leuven*.

Earls Davis, P. A. (2020). Facial Detection and Smart Billboards: Analysing the 'Identified' Criterion of Personal Data in the GDPR. *European Data Protection Law Review*, *6*, 365.

El Khoury, A. (2018). Personal Data, Algorithms and Profiling in the EU: Overcoming the Binary Notion of Personal Data through Quantum Mechanics. *Erasmus Law Review*, *11*, 172.

Elliot, M., O'hara, K., Raab, C., O'Keefe, C. M., Mackey, E., Dibben, C., ... & McCullagh, K. (2018). Functional anonymisation: Personal data and the data environment. *Computer Law & Security Review*, *34*(2), 204-221.

Esayas, S. (2015). The role of anonymisation and pseudonymisation under the EU data privacy rules: beyond the 'all or nothing' approach. *European Journal of Law and Technology*, *6*(2), 3.

Espinoza, J (2021, March 4). EU data protection laws need overhaul, says policy architect; GDPR. *Financial Times (London, England).* Retrieved from https://advance-lexis-com.vu-nl.idm.oclc.org/api/document?collection=news&id=urn:contentItem:624G-V5C1-DYTY-C3DR-00000-00&context=1516831.

European Commision (n.d.). A European Strategy for data. Retrieve from https://digital-strategy.ec.europa.eu/en/policies/strategy-data

European Commission (2020). Proposal for a Regulation on European data governance (Data Governance Act), COM/2020/767 final.

European Commission (n.d.). Smart cities. Retrieved from https://commission.europa.eu/eu-regional-and-urban-development/topics/cities-and-urban-development/city-initiatives/smart-cities_en

European Commission. (2010). Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Youth Opportunities Initiative: 'A comprehensive approach on personal data protection in the European Union'. *COM(2010) 609 final*. Retrieved from https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0609:FIN:EN:PDF

European Data Protection Supervisor (2018). Opinion 5/2018–Preliminary Opinion on Privacy by Design. Retrieved from https://edps.europa.eu/

European Union Agency for Fundamental Rights (2018). Chapter 2: Data protection terminology (pp. 22). In *Handbook on European Data Protection Law*.

European Union Agency for Fundamental Rights and Council of Europe (2018). Handbook on European data protection law. *Fra.europa.eu*. Retrieved from https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf

European Union Agency for Network and Information Security (ENISA) (2017). Handbook on Security of Personal Data Processing. *ENISA*.

Figueiredo, S. M., & Agyin, J. (2019). Hidden in plain sight: Toward a smart future in Eindhoven. *Architecture and Culture*, *7*(3), 493-504.

Finck, M., & Pallas, F. (2020). They who must not be identified—distinguishing personal from non-personal data under the GDPR. *International Data Privacy Law*, *10*(1), 11-36.

Fischer, C. (2020). The legal protection against inferences drawn by AI under the GDPR [L.L.M. thesis]. *Tilburg Law School, LL.M. Law and Technology.*

Floridi, L. (2005). Is semantic information meaningful data?. *Philosophy and phenomenological research*, *70*(2), 351-370.

Franke, J., & Gailhofer, P. (2021). Data governance and regulation for sustainable smart cities. *Frontiers in Sustainable Cities*, *3*, 148.

Fuster, G. G. (2014). *The emergence of personal data protection as a fundamental right of the EU* (Vol. 16) (pp. 214). Springer Science & Business.

Galdon-Clavell, G. (2013). (Not so) smart cities?: The drivers, impact and risks of surveillance-enabled smart environments. *Science and Public Policy*, *40*(6), 717-723.

Galič, M. (2019). *Surveillance and privacy in smart cities and living labs: Conceptualising privacy for public space* [PhD-Thesis – Research and graduation external, Tilburg University]. Optima Grafische Communicatie.

Galič, M. (2019). Surveillance, privacy and public space in the Stratumseind Living Lab: The smart city debate, beyond data. *Ars Aequi, special issue July/August*.

Galič, M., & Gellert, R. (2021). Data protection law beyond identifiability? Atmospheric profiles, nudging and the Stratumseind Living Lab. *Computer Law & Security Review*, *40*, 105486.

Gellert, R. (2021). Personal data's ever-expanding scope in smart environments and possible path(s) for regulating emerging digital technologies. *International Data Privacy Law*, 11(2), 196–208.

Gellert, R. (2022). Comparing definitions of data and information in data protection law and machine learning: A useful way forward to meaningfully regulate algorithms?. *Regulation & Governance*, *16*(1), 156-172.

Geradin, D., Karanikioti, T., & Katsifis, D. (2021). GDPR Myopia: how a well-intended regulation ended up favouring large online platforms-the case of ad tech. *European Competition Journal*, *17*(1), 47-92.

Graef, I., & Van Der Sloot, B. (2022). Collective data harms at the crossroads of data protection and competition law: Moving beyond individual empowerment. *European Business Law Review*, *33*(4), 513-536.

Graef, I., Gellert, R., & Husovec, M. (2018). *Towards a holistic regulatory approach for the European data economy: Why the illusive notion of non-personal data is counterproductive to data innovation*. (TILEC Discussion Paper Series; Vol. 2018, No. 29) (pp. 7).

Graef, I., Gellert, R., Purtova, N., & Husovec, M. (2018). Feedback to the Commission's Proposal on a Framework for the Free Flow of Non-Personal Data. *SSRN Electronic Journal,* 3.

Groos, D., & van Veen, E. B. (2020). Anonymised data and the rule of law. *Eur. Data Prot. L. Rev.*, *6*, 498.

Gstrein, O. J., & Ritsema van Eck, G. J. (2018). Mobile devices as stigmatizing security sensors: The GDPR and a future of crowdsourced ‘broken windows.’ *International Data Privacy Law, 8*(1), 80–81.

Hajduk, P. (2021). The Powers of the Supervisory Body in the GDPR as Basis for Shaping the Practices of Personal Data Processing. *Review of European and Comparative Law (RECoL)*, 45, 57-76.

Hallinan, D. & Gellert, R.M. (2020). The Concept of 'Information'. An Invisible Problem in the GDPR. Script-Ed, 17 (2), 269-319.

Heidegger, M. (1977) The Question Concerning Technology, in: *The Question Concerning Technology and Other Essays*,W. Lovitt (trans.) (New York, Harper and Row), pp. 3– 35.

Hildebrandt, M. (2006). Profiling: From data to knowledge: The challenges of a crucial technology. *Datenschutz und Datensicherheit-DuD*, *30*(9).

Hildebrandt, M. (2013). Slaves to Big Data. Or are we?. *IDP Revista De Internet, Derecho Y Política.*

Hildebrandt, M. (2015). *Smart technologies and the end (s) of law: novel entanglements of law and technology.* Edward Elgar Publishing.

Hildebrandt, M. (2016). Law as Information in the Era of Data Driven Agency. *The Modern Law Review*, *79*(1), 1-30.

Hildebrandt, M., & Tielemans, L. (2013). Data protection by design and technology neutral law. *Computer Law & Security Review*, *29*(5), 509-521.

Hintze, M. (2018). Viewing the GDPR through a de-identification lens: a tool for compliance, clarification, and consistency. *International Data Privacy Law*, *8*(1), 86-101.

Hon, W. K., Millard, C., & Walden, I. (2011). The problem of 'personal data' in cloud computing: what information is regulated?—the cloud of unknowing. *International Data Privacy Law*, *1*(4), 211-228.

Hondius, F. W. (1975). *Emerging data protection in Europe*. Amsterdam: North-Holland Publishing Company; New York: American Elsevier Publishing Company.

International Organization for Standardization (2018, February) ISO 31000:2018 Risk management – Guidelines. (February 2018). Retrieved from https://www.iso.org/standard/65694.html

Irti, C. (2022). Personal Data, Non-personal Data, Anonymised Data, Pseudonymised Data, De-identified Data. In: Senigaglia, R., Irti, C., Bernes, A. (eds) *Privacy and Data Protection in Software Services. Services and Business Process Reengineering*. Springer, Singapore.

Ivanova, Y. (2021). The Role of the EU Fundamental Right to Data Protection in an Algorithmic and Big Data World. *Data Protection and Privacy: Data Protection and Artificial Intelligence*, 809, 145.

Janeček, V. (2018). Ownership of personal data in the Internet of Things. *Computer law & security review*, *34*(5), 1039-1052.

Jasmontaite, L., Kamara, I., Zanfir Fortuna, G., & Leucci, S. (2018). Data protection by design and by default: Framing guiding principles into legal obligations in the GDPR. *European Data Protection Law Review*, *4*(2), 168-189.

Jastroch, N. (2020). Trusted artificial intelligence: on the use of private data. In *Product Lifecycle Management Enabling Smart X: 17th IFIP WG 5.1 International Conference, PLM 2020, Rapperswil, Switzerland, July 5–8, 2020, Revised Selected Papers 17* (pp. 659-670). Springer International Publishing.

Jiang, H., Geertman, S., & Witte, P. (2022). The contextualization of smart city technologies: An international comparison. *Journal of Urban Management*.

Johnson, J., Hevia, A., Yergin, R., Karbassi, S., Levine, A., & Ortiz, J. (2022). Data governance frameworks for smart cities: key considerations for data management and use. *Journal of Law and Mobility*, *2022*(1), 1.

Kaluarachchi, Y. (2022). Implementing data-driven smart city applications for future cities. *Smart Cities*, *5*(2), 455-474.

Koops, B. J. (2014). The trouble with European data protection law. *International data privacy law*, *4*(4), 250-261.

Koops, B. J. (2021). The concept of function creep. Law*, Innovation and Technology, 13*(1), 29-56.

Koops, E. J. (2006). Should ICT Regulation Be Technology-Neutral? In B. J. Koops, A. M. B. Lips, J. E. J. Prins, & M. H. M. Schellekens (Eds.), *Starting Points for ICT Regulation* (pp. 82-85). (Information Technology and Law Series, No. 9). The Hague: T.M.C. Asser Press.

Korff, D., & Shadbolt, N. (2010). Public information: Cause for celebration or concern?. *Public and Science*, 10-11.

Kröger, J. (2019). Unexpected Inferences from Sensor Data: A Hidden Privacy Threat in the Internet of Things. In L. Strous and V. G. Cerf *(*Eds.), *Internet of Things. Information Processing in an Increasingly Connected World* (pp. 147–159). Cham: Springer.

Kröger, J. L. (2022). *Rogue Apps, Hidden Web Tracking and Ubiquitous Sensors* [Doctoral dissertation, Universität Berlin], 222–225.

Kröger, J. L., Lutz, O. H. M., Müller, F. (2020). What Does Your Gaze Reveal About You? On the Privacy Implications of Eye Tracking. In Friedewald, M., Önen, M., Lievens, E., Krenn, S., Fricker, S. (Eds.), *Privacy and Identity Management. Data for Better Living: AI and Privacy. Privacy and Identity*. IFIP Advances in Information and Communication Technology (Vol. 576. pp. 226–241).

Kröger, J. L., Miceli, M., & Müller, F. (2021). How data can be used against people: a classification of personal data misuses [Preprint]. *Available at SSRN 3887097*.

Kuner, C. (2012). The European Commission's proposed data protection regulation: A copernican revolution in European data protection law. *Bloomberg BNA Privacy and Security Law Report (2012) February*, *6*(2012), 1-15l.

LAST-JD-RIoE (2021). Processing of home data in the light of the GDPR and IPR issues. *Law, Science and Technology Joint Doctorate: Rights of the Internet of Everything (LAST-JD-RIoE)*.

Lazaro, C., & Metayer, D. L. (2015). Control over personal data: True remedy or fairy tale. *SCRIPTed*, *12*.

Lee, J., Babcock, J., Pham, T. S., Bui, T. H., & Kang, M. (2023). Smart city as a social transition towards inclusive development through technology: a tale of four smart cities. *International Journal of Urban Sciences*, *27*(sup1), 75-100.

Leiser, M. R., & Dechesne, F. (2020). Governing machine-learning models: challenging the personal data presumption. *International Data Privacy Law, 10*(3), 187.

Lukas, L. L., & Arnold, J. F. (2023). Machine Data, Personal Data, Sensitive Data and Artificial Intelligence. the Interplay of Privacy Enhancing Technologies with the GDPR. Available at SSRN: https://ssrn.com/abstract=4341844

Mai, J.-E. (2016). Big data privacy: The datafication of personal information. *The Information Society, 32*(3), 192–199.

Mantelero, A. (2017). Regulating big data. The guidelines of the Council of Europe in the context of the European data protection framework. *Computer law & security review*, *33*(5), 584-602.

McDonald, A. M., & Cranor, L. F. (2008). The cost of reading privacy policies. *Isjlp*, *4*, 543.

Mildebrath, H. (2022). Understanding EU data protection policy. *European Parliamentary Research Service*.
https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/698898/EPRS_BRI(2022)698898_EN.pdf

Moerel, L. (2014). Big Data Protection. How to Make the Draft EU Regulation on Data Protection Future Proof. How to Make the Draft EU Regulation on Data Protection Future Proof. *Tilburg Institute for Law, Technology, and Society.*

Moerel, L., & Prins, C. (2016). Privacy for the homo digitalis: Proposal for a new regulatory framework for data protection in the light of Big Data and the internet of things, 12.

Moiny, J. P., De Terwangne , C., Van Gyseghem, J. M., & Poullet, Y. (2010). *Rapport sur les lacunes de la Convention n° 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel face aux développements technologiques (Partie II)*. Conseil de l'Europe.

Narayanan, A., & Shmatikov, V. (2010). Myths and fallacies of" personally identifiable information". *Communications of the ACM*, *53*(6), 24-26.

OECD (2019). Enhancing The Contribution Of Digitalisation To The Smart Cities Of The Future. Retrieved from https://www.oecd.org/cfe/regionaldevelopment/Smart-Cities-FINAL.pdf

Ohm, P. (2009). Broken promises of privacy: Responding to the surprising failure of anonymization. *UCL Law Review*, *57*, 1701-1777.

Ohm, P., & Peppet, S. (2016). What If Everything Reveals Everything?. *Big Data Is Not a Monolith (MIT Press 2016)*.

Omotubora, A., & Basu, S. (2020). Next generation privacy. *Information & Communications Technology Law*, *29*(2), 151-173.

Pan, J., & Yang, Z. (2018, March). Cybersecurity challenges and opportunities in the new "Edge Computing+ IoT" world. In *Proceedings of the 2018 ACM International Workshop on Security in Software Defined Networks & Network Function Virtualization* (pp. 29-32).

Pereira, G. V., Parycek, P., Falco, E., & Kleinhans, R. (2018). Smart governance in the context of smart cities: A literature review. Information Polity, 23(2), 143-162.

Podda, E. (2021) Shedding light on the legal approach to aggregate data under the GDPR & the FFDR [CONFERENCE OF EUROPEAN STATISTICIANS - Expert Meeting on Statistical Data Confidentiality]. *UNEC*. Retrieved on 22 November 2022 from https://unece.org/sites/default/files/2021-12/SDC2021_Day1_Podda_AD.pdf

Podda, E., & Palmirani, M. (2020). Inferring the Meaning of Non-personal, Anonymized, and Anonymous Data. In *AI Approaches to the Complexity of Legal Systems XI-XII* (pp. 269-282). Springer, Cham.

Politou, E., Alepis, E., & Patsakis, C. (2018). Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions. *Journal of cybersecurity*, *4*(1), 3.

Purtova, N (2017). Do property rights in personal data make sense after the Big Data turn? Individual control and transparency. *Tilburg Law School Research Paper No. 2017/21*, 13–17.

Purtova, N. (2018). The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, *10*(1), 40-81.

Purtova, N. (2020). Code as personal data. *INFO-LEG* [working paper], 1-14. *Available at SSRN 3786673*

Purtova, N. (2020). Organising concepts in law: a typology and lessons for data protection. *INFO-LEG.*

Purtova, N. (2022). From knowing by name to targeting: the meaning of identification under the GDPR. *International Data Privacy Law*, *12*(3), 163-183.

Quach, S., Thaichon, P., Martin, K. D., Weaven, S., & Palmatier, R. W. (2022). Digital technologies: Tensions in privacy and data. *Journal of the Academy of Marketing Science*, *50*(6), 1299-1323.

Quinn, P. (2021). The Difficulty of Defining Sensitive Data—The Concept of Sensitive Data in the EU Data Protection Framework. *German Law Journal, 22*(8), 1569.

Reidenberg, J. R. (1999). Resolving conflicting international data privacy rules in cyberspace. *Stanford Law Review*, *52*, 1315.

Remac, M. (2017). The European Union Agency for Network and Information Security (ENISA)-Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA).

Rhoen, M. H. C. (2019). *Big data, big risks, big power shifts: Evaluating the General Data Protection Regulation as an instrument of risk control and power redistribution in the context of big data*. [PhD-Thesis – Research and graduation external, Leiden University].

Romansky, P. R., & S. Noninska, I. (2020). Challenges of the digital age for privacy and personal data protection. *Mathematical Biosciences and Engineering,* 17(5), 5288–5303.

Saglam, R. B., Nurse, J. R., & Hodges, D. (2022). Personal information: Perceptions, types and evolution. *Journal of Information Security and Applications*, *66*, 103163.

Scholl, H. J., & AlAwadhi, S. (2016). Creating Smart Governance: The key to radical ICT overhaul at the City of Munich. *Information Polity*, *21*(1), 22.

Schwartz, P. M., & Solove, D. J. (2011). The PII problem: Privacy and a new concept of personally identifiable information. *NYUL rev.*, *86*, 1814.

Skiljic, A. (2021, March 19). The status quo of health data inferences. *iapp.org*. Recruited from: https://iapp.org/news/a/the-statusquo-of-health-data-inferences/

Søe, S. O. (2021). Non-natural Personal Information. Accounting for Misleading and Non-misleading Personal Information. *Philosophy & Technology*.

Søe, S. O., Jørgensen, R. F., & Mai, J. E. (2021). What is the 'personal' in 'personal information'?. *Ethics and Information Technology,* 23(4), 625-633.

Solove, D. J. (2010). Fourth amendment pragmatism. *Boston College Law Review*, *51*, 1511-1538.

Solove, D. J. (2023). Data Is What Data Does: Regulating Use, Harm, and Risk Instead of Sensitive Data. *Harm, and Risk Instead of Sensitive Data* (pp. 45-48).

Solove, D. J., & Hartzog, W. (2021). *Breached!*. Oxford University Press.

Stalla-Bourdillon, S., & Knight, A. (2016). Anonymous data v. personal data-false debate: an EU perspective on anonymization, pseudonymization and personal data. *Wisconsin International Law, 34*, 284.

Stamp, M. (2011). *Information security: principles and practice* (pp. 2). John Wiley & Sons.

Stefanouli, M., & Economou, C. (2018). Data protection in smart cities: Application of the EU GDPR. In *Conference on Sustainable Urban Mobility* (pp. 748-755). Springer, Cham.

Stenudd, S. (2011, May). A model for using machine learning in smart environments. In *International Conference on Grid and Pervasive Computing* (pp. 24-33). Springer, Berlin, Heidelberg.

Strate, L. (2012). If it's neutral, it's not technology. *Educational Technology*, 6-9.

Sweeney, L. (2000). Simple demographics often identify people uniquely. *Health (San Francisco)*, *671*(2000), 1-34.

Talebkhah, M., Sali, A., Marjani, M., Gordan, M., Hashim, S. J., & Rokhani, F. Z. (2021). IoT and big data applications in smart cities: recent advances, challenges, and critical issues. *IEEE Access*, *9*, 55465-55484.

Taylor, L., Floridi & B. Van Der Sloot (2017). *Group privacy: New challenges of data technologies* (Vol. 126).

Tene, O., & Polonetsky, J. (2012). Big data for all: Privacy and user control in the age of analytics. *Northwestern Journal of Technology and Intellectual Property,11*, 258.

Terstegge, J. (2020, February 4), Do we need a new GDPR? *NetKwesties*. Retrieved from https://www.netkwesties.nl/1421/do-we-need-a-new-gdpr.htm

Tzanou, M. (2020). The GDPR and (big) health data: Assessing the EU legislator’s choices. In *Health Data Privacy under the GDPR* (pp. 3-22). Routledge.

Tzanou, M. (2021). Data Protection/Data Privacy. *Encyclopaedia entry, in Elgar Encyclopaedia of Human Rights, Forthcoming*, 6.

Ufert, F. (2020). AI regulation through the lens of fundamental rights: How well does the GDPR address the challenges posed by AI?. *European Papers-A Journal on Law and Integration*, *2020*(2), 1087-1097.

Van Der Sloot, B. (2017). Do groups have a right to protect their group interest in privacy and should they? Peeling the onion of rights and interests protected under article 8 ECHR. *Group privacy: new challenges of data technologies*, 197-224.

Van Der Sloot, B. (2017). *Privacy as virtue*. Intersentia.

Van Der Sloot, B. (2020). Regulating non-personal data in the age of Big Data. In *Health Data Privacy under the GDPR* (pp. 85-105). Routledge.

Van Der Sloot, B. (2021). The right to be let alone by oneself: Narrative and identity in a data-driven environment. *Law, Innovation and Technology*, *13*(1), 223-255.

Van Der Sloot, B. & & Zuiderveen Borgesius, F. J. (n.d.). The Eu General Data Protection Regulation: A New Global Standard For Information Privacy [*Working draft*]. Retrieved from https://bartvandersloot.com/onewebmedia/SSRN-id3162987.pdf

Van der Sloot, B., & Keymolen, E. (2022). Can we trust trust-based data governance models?. *Data & Policy*, *4*, 45.

Van Der Sloot, B., & Lanzing, M. (2021). The continued transformation of the public sphere: on the road to smart cities, living labs and a new understanding of society. *Technology and the City: Towards a Philosophy of Urban Technologies*, 319-345.

Van der Sloot, B., & Van Schendel, S. (2021). Procedural law for the data-driven society. *Information & Communications Technology Law*, *30*(3), 304-332.

Van der Sloot, B., Van Schendel, S., & López, C. A. F. (2022). The influence of (technical) developments on the concept of personal data in relation to the GDPR. *TILT – Tilburg Institute of Law, Technology, and Society*.

Van Lieshout, M. (2016). Privacy and Innovation: From Disruption to Opportunities. *Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection*, 195-212.

Van Loenen, B., Kulk, S., & Ploeger, H. (2016). Data protection legislation: A very hungry caterpillar: The case of mapping data in the European Union. *Government Information Quarterly*, *33*(2), 338-345.

Van Zoonen, L. (2016). Privacy concerns in smart cities. *Government Information Quarterly*, *33*(3), 472-480.

Vardanyan, L., & Kocharyan, H. The GDPR and the DGA Proposal: are They in Controversial Relationship?. *European Studies*, *9*(1), 91-109.

Veale, M., Binns, R., & Edwards, L. (2018). Algorithms that remember: model inversion attacks and data protection law. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, *376*(2133), 8.

Vojković, G., & Katulić, T. (2020). Data protection and smart cities. *Handbook of smart cities*, 1-26.

Voss, W. G. (2019). Cross-border data flows, the GDPR, and data governance. *Washington International Law Journal*, *29*, 485.

Vranken, J. (2012). Exciting times for legal scholarship. *Law and method*, *2*(2), 42-62.

Wachter, S. (2018). Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR. *Computer law & security review*, *34*(3), 436-449.

Wachter, S., & Mittelstadt, B. (2019). A right to reasonable inferences: re-thinking data protection law in the age of big data and AI. *Colum. Bus. L. Rev., 2019*(2), 521-531.

Waerdt, van de, P. (2020). Information asymmetries: recognizing the limits of the GDPR on the data-driven market. Computer Law & Security Review, 38, [105436], 12

Waldman, A. E. (2020). Data Protection by Design? A Critique of Article 25 of the GDPR. *Cornell International Law Journal, 53*, 147.

Weitzenboeck, E. M., Lison, P., Cyndecka, M., & Langford, M. (2022). The GDPR and unstructured data: is anonymization possible?. *International Data Privacy Law*, *12*(3), 184-206.

Wong, B. (2019). Delimiting the concept of personal data after the GDPR. *Legal Studies*, *39*(3), 517-532.

Zangrandi, R. (n.d.) I'm sorry my Friend, but you're Implicit in the Algorithm. Privacy and Internal Access to Big Data Stream: An Interview with Giovanni Buttarelli. *European Data Protection Supervisor.* Retrieved from https://edps.europa.eu/data-protection/our-work/publications/articles/%E2%80%98i%E2%80%99m-sorry-my-friend-you%E2%80%99re-implicit-algorithm%E2%80%A6%E2%80%99_en

Zarsky, T. Z. (2016). Incompatible: The GDPR in the age of big data. *Seton Hall Law Review*, *47*, 995-1020.

Zhao, B., & Chen, W. (2019). Data protection as a fundamental right: The European General Data Protection Regulation and its exterritorial application in China. *US-China Law Review*, 16, 97, 99.