D 1.5

Enforcing responsibilities in Smart Cities

Deliverable Title	Enforcing responsibilities in Smart Cities
Deliverable Number	D1.5
Authors	Athena Christofi, Olia Kanevskaia
Editor	Ellen Wauters

This document forms part of the 'SPECTRE' (**S**mart city **P**rivacy: **E**nhancing **C**ollaborative **T**ransparency in the **R**egulatory **E**cosystem) project. SPECTRE is a four-year interdisciplinary research project funded by FWO (Flanders Research Foundation). The main goal is to *examine* privacy and data protection challenges in the smart city from legal, social sciences and economic perspectives and to *propose solutions* to address the privacy/utility challenge that more and more cities are called to face. Solutions will focus on:

- Improving legal compliance by looking into (legal) tools within and beyond the GDPR;
- Making smart-city Data Protection Impact Assessments participatory and collaborative, so as to enhance data protection and societal acceptance of the proposed smart-city innovations;
- Understanding broader considerations that may influence the development of smart cities, notably the costs of Data Protection Impact Assessments / of data protection more generally and the impact of data concentrations on competition and data protection.

The SPECTRE consortium comprises of the following partners:

- KU Leuven: Research group Centre for IT and IP Law (CiTiP)
- Free University Brussels: Research groups Studies in Media, Innovation and Technology (SMIT), Business and Applied Economics (BUSI-APEC)

For more information in relation to the project, visit our website https://spectreproject.be/.

Please cite the following:

Athena Christofi and Olia Kanevskaia (2021) 'Enforcing responsibilities in Smart Cities'. A report in the framework of the SPECTRE research project. Document accessible at https://spectreproject.be/.

TABLE OF CONTENT

List of Abbreviations

CFR	European Charter of Fundamental Rights
CJEU	Court of Justice of the European Union
DPA	Data Protection Authority
DPIA	Data Protection Impact Assessment
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
GDPR	General Data Protection Regulation
IA	Impact Assessment
WP29	Article 29 Data Protection Working Party

INTRODUCTION

Data is crucial for smart city services. More often than not, the functioning of smart cities hinges on the collection, processing and storing of personal data, which subjects smart cities services to the General Data Protection Regulation (GDPR) of the European Union. However, compliance with the GDPR requirements is increasingly difficult in the smart city environment due to the technical and legal complexities as well as power imbalances between smart cities actors.

This deliverable explores whether and how does the risk-based approach of the GDPR affect the enforcement of data protection in the smart city environment. The term 'enforcement', used in the deliverable, broadly describes the evaluation, monitoring and supervision of data protection. We examine whether the current shift from command and control to decentralized regulation upon the introduction of the GDPR could weaken data protection enforcement in smart cities rather than strengthen it. In particular, we suggest that by placing a greater accountability burden on controllers, the regulatory approach used by the GDPR has created an accountability gap between data subjects and entities involved in the different stages of data processing, and that the instruments and mechanisms provided in the GDPR do not sufficiently compensate for the resulting challenges of accountability and legitimacy.

This deliverable is structured as follows. Section 1 contains a brief discussion of the regulatory nature of the GDPR, and explains the role of the accountability principle and of the risk-based approach in EU data protection law. Section 2 describes the key enforcement mechanisms provided in the GDPR, and distils the main challenges resulting from the decentralization of the application and enforcement of data protection law. Section 3 then views these and additional challenges in the context of smart cities environment, focusing on the issues of the complex rights that may be at stake at the city environment and the difficulty to identify and understand risks; the challenge of assessing cumulative effects on fundamental rights possibly arising through the slow development of different smart city projects; and accountability deficits created by the involvement of private entities in the design and deployment of smart city initiatives. With these challenges in mind, we conclude by proposing different theoretical frameworks that could legitimize and enhance data protection rights in smart cities, and pave the way for concretizing these frameworks in a further research, to be followed in Deliverables 1.6 and 4.7.

1 ACCOUNTABILITY AND RISK: INTRODUCING THE GDPR'S REGULATORY NATURE

1.1 A hybrid ''rule-based'' and ''principle-based'' model

REGULATORY STRATEGIES. Regulation has famously been defined by Selznick as the "sustained and focused control exercised by a public agency over activities that are valued by a community".[1] It usually involves the promulgation of a binding set of rules, which aim to prevent certain undesirable activities from happening (by restricting certain behaviours), or, to enable or facilitate certain activities to take place in an ordered way.[2] States, and in the case of EU, supranational entities can choose among a number of different regulatory strategies or techniques when deciding to regulate. Two techniques are particularly relevant to discuss in the data protection context: "command and control" and "meta-regulation".

"Command and control" denotes what is often characterized as "classical regulation", whereby laws set clear fixed rules that prescribe prohibitions or conditions for the exercise of an activity, and back such rules with sanctions and legal redress.[3] While setting clear and generally applicable rules reduces uncertainty, "command and control" regulation is not without challenges. A key criticism lies to the inability of rigid rules to provide the flexibility needed to accommodate fast-paced social and technological change.[4] There is also a risk that regulated entities view the rules solely as minimum compliance targets and lose incentives to improve and change their behavior so that it goes beyond such minimum compliance.[5]

With meta-regulation, certain regulatory functions are delegated to the regulated entities themselves. Laws and the regulatory authorities created to oversee compliance "steer" and "monitor" rather than strictly prescribe certain behaviours.[6] Regulated entities then become responsible to control the risks of their behaviour, leveraging their existing management structures, knowledge and

[1] Philip Selznick, 'Focusing Organizational Research on Regulation' in Roger Noll (ed), *Regulatory Policy and the Social Sciences* (University of California Press 1985) 383.

[2] Robert Baldwin, Martin Cave and Martin Lodge, *Understanding Regulation: Theory, Strategy, and Practice* (2nd Edition, Oxford University Press 2012) 3.

[3] ibid 106–110.

[4] Athena Christofi and others, 'Erosion by Standardisation: Is ISO/IEC 29134:2017 on Privacy Impact Assessment Up to (GDPR) Standard?' in Maria Tzanou (ed), *Personal Data Protection and Legal Developments in the European Union* (IGI Global 2020) 141.

[5] Martin Lodge and Kai Wegrich, *Managing Regulation: Regulatory Analysis, Politics and Policy* (Palgrave Macmillan 2012) 97.

[6] Baldwin, Cave and Lodge (n 2) 147.

"inherent capacity to manage themselves".[7] The said benefits of this approach compared to "command and control" regulation is that organisations are given the flexibility, freedom and incentives to come up with protection measures that are tailored to their mode of operating. Because rules are tailored, they can arguably produce better results than uniform rules, which risk to be too demanding for some entities while too lax for others. It has also been argued that when regulated entities are asked to think for themselves about the risks and impacts of their behaviour, this can increase their consciousness and change corporate cultures.[8] Nevertheless, while meta-regulation relies in the capacity and commitment of regulated entities to self-regulate in the public interest, it is important to acknowledge that such entities could be "ill-intentioned, ill-informed, or inefficient" and fail to devise the appropriate rules needed to protect the public interest.[9] Without appropriate monitoring and supervision from regulatory authorities, there is a risk that it leads to a race to the bottom.

CHALLENGES OF REGULATING PERSONAL DATA PROCESSING. Personal data processing is a complex activity to regulate in a way that ensures protection against the risks, while enabling processing in an era when it is admittedly indispensable. A first challenge relates to the law's pacing problem. Data processing technologies are fast evolving, constantly presenting new risks but also opportunities. As pointedly put by Downes, "while technology changes exponentially, social, economic and legal systems change incrementally".[10] It is challenging for regulators to enact a future-proof framework which both addresses all risks and enables innovation. Secondly, since the enactment of the first EU-wide data protection legislation (Directive 95/46/EC), the EU legislator has opted for an omnibus regime, which is sector- and technology- neutral, and applies to both private and public authorities.[11] Such a catch-all regime provides coherence and a high level of protection across different sectors. At the same time, it is important to allow for some flexibility. Data protection legislation should be fit for purpose to regulate activities as diverse as the extensive profiling for assessing a person's creditworthiness or movement patterns within a city, and the sending of a small company's promotional catalogue to its customers.[12] A rule-based approach setting prescriptive rules would risk setting disproportionate standards on organisations where the processing of personal data is an incidental

[7] Reuben Binns, 'Data Protection Impact Assessments: A Meta-Regulatory Approach' (2017) 7 International Data Privacy Law 22, 23.

[8] Baldwin, Cave and Lodge (n 2) 148.

[9] ibid 150.

[10] Larry Downes, *The Laws of Disruption: Harnessing the New Forces That Govern Life and Business in the Digital Age* (Basic Books 2009) 2.

[11] Orla Lynskey, *The Foundations of EU Data Protection Law* (2015) 15–30.

[12] Christofi and others (n 4) 143.

and/or low-risk activity. Or, to avoid such a situation, it could end up setting minimum requirements that might offer limited protection against complex and risky processing operations.[13]

THE GENERAL DATA PROTECTION REGULATION. In light of the challenges described above, the GDPR essentially follows a hybrid approach with characteristics of both "command and control" rule-based regulation and meta-regulation based on broad principles. As "hard law" containing mandatory legal requirements and backed up with monitoring and enforcement mechanisms, as well remedies and sanctions in case of violation, it embraces the traditional "command and control" approach.[14] Among its legal requirements, some are in fact very prescriptive. The provisions on controller-processor agreements and records of processing activities are cases in point. At the same time, the GDPR largely follows a principle-based approach and has the characteristics of meta-regulation. At the core of the GDPR are the data protection principles set forth in Article 5, namely: lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality. Their interpretation and application depends on a case-by-case analysis by controllers, taking into consideration the specific circumstances and risks of a processing operation.[15] Controllers are thus entrusted with important decision-making powers. They are called to decide, for instance, how to ensure the fairness of processing, when is processing necessary in relation to a specific purpose or interest, or when a new processing purpose is (in)compatible with the initial purpose.[16] In view of these broad principles, the GDPR in fact relies heavily on the active participation of controllers in setting standards (by interpreting and applying principles) and managing the risks of their processing operations.[17] This active participation and delegation of power reminisces "meta-regulation".

1.2 The risk-based approach

THE ROLE OF RISK IN THE GDPR. The GDPR has made "risk" a central notion in the data protection framework. The so called risk-based approach in the GDPR entails the following. The risk presented by the data processing to the "rights and freedoms of individuals" acts as a yardstick to tailor controllers' obligations,

[13] Ibid.

[14] Karen Yeung and Lee A Bygrave, 'Demystifying the Modernized European Data Protection Regime: Cross-Disciplinary Insights from Legal and Regulatory Governance Scholarship' Regulation & Governance 5.

[15] Christofi and others (n 4) 145.

[16] ibid.

[17] Yeung and Bygrave (n 14) 5.

establishing a scalable approach to compliance.[18] For instance, certain (admittedly burdensome) legal requirements in the GDPR are only triggered in case the processing presents a high risk: Data Protection Impact Assessments (Art. 35) and the obligation for prior consultation of the Data Protection Authority (Art. 36) are cases in point. Most importantly though, Article 24 –a core provision setting forth the responsibility of controllers- also embraces a risk-based approach. The provision requires controllers to implement appropriate technical and organizational measures to ensure and be able to demonstrate that the processing is in accordance with the Regulation. The appropriateness of such measures is to be determined "[t]aking into account the nature, scope, context and purposes of processing *as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons*". In essence, the higher the risks, the more extensive are the obligations of controllers to ensure that risks and possible negative impacts on individuals are addressed.

A RIGHTS-BASED AND RISK-BASED APPROACH. Being a fundamental right, the right to data protection should apply irrespective of the risk of a processing operations and provide a minimum and non-negotiable level of protection for all individuals.[19] Hence, following such "rights-based" approach, full compliance with data protection law should always take place. This has been emphasized by Article 29 Working Party (WP29) in its statement on the role of a risk-based approach in data protection legal frameworks.[20] According to it, the data subjects rights recognized in data protection law (e.g. access, rectification, objection) apply and should be respected regardless of the level of risk. Similarly, the fundamental principles of Article 5 GDPR should remain the same regardless of the nature and risks of the processing. Therefore, the risk-based approach is not an alternative to established data protection principles and rights (i.e. the "rights-based" approach) but *adds* to them.[21] As WP29 explains, implementation of certain obligations, such as data protection impact assessments, data protection by design, security measures, should be scalable and varied depending on the type of processing and its risks for data subjects.[22] Such an approach "ensures the

[18] Milda Macenaite, 'The "Riskification" of European Data Protection Law through a Two-Fold Shift' (2017) 8 European Journal of Risk Regulation 506, 517.

[19] Raphaël Gellert, 'Understanding the Notion of Risk in the General Data Protection Regulation' (2018) 34 Computer Law & Security Review 279, 282.

[20] Article 29 Data Protection Working Party, 'Statement on the Role of a Risk-Based Approach in Data Protection Legal Frameworks' (2014) WP 218.

[21] Gellert (n 19) 283.

[22] Article 29 Data Protection Working Party, 'Statement on the Role of a Risk-Based Approach in Data Protection Legal Frameworks' (n 20) 3.

flexibility necessary to go from a rigid to a scalable regulatory framework able to encompass a wide variety of different situations".[23]

RISK TO WHAT? The risks with which the GDPR is preoccupied, and against which it seeks to ensure protection, are the possible risks of processing operations to the "rights and freedoms" of individuals.[24] WP29 has again clarified that the right at stake is not only privacy but also other fundamental rights such as freedom of speech, freedom of thought, and prohibition of discrimination.[25] Academic literature considers that the concept of "rights and freedoms" encompasses the whole European fundamental rights framework, notably the rights recognised in the European Convention on Human Rights (ECHR) and the EU Charter of Fundamental Rights (CFR).[26] Such an approach is indeed in line with the objective of the GDPR to protect fundamental rights and freedoms of individuals, in particular (but not only) their right to data protection.[27] It also entails that assessments of risks go further than "ticking the box" exercises of compliance with specific provisions of the Regulation such as data security.

THE COMPLEXITY OF THE "RISKS TO RIGHTS" CONCEPT. Even though it is clear that the GDPR specifically refers to risks to rights and freedoms, how fundamental rights considerations can be embedded into traditional risk assessment processes is particularly complex. The concept of "risks to rights" is a conceptual legal novelty and challenge given that "risks and rights traditionally belong to different spheres of knowledge and social organisation".[28]

Risk management encompasses the tools, process and methods used to make decisions as to whether or not to take a risk, and how to reduce such risk.[29] It generally requires the decision-maker at stake to set certain risk criteria and identify risks, to then conduct the proper risk assessment and management. As risk are "feared events" that may or may not occur in the future, risks assessments are anticipatory exercises. The risk management assessment involves, once risks have been identified, "the balancing of the costs and benefits associated [to the risks]" and a decision on whether or not to take such risks.[30] If taking the risks is

[23] Christofi and others (n 4) 145.

[24] See Recitals 75 & 76, as well as Articles 24, 25, 35 and 36 GDPR.

[25] Article 29 Data Protection Working Party, 'Statement on the Role of a Risk-Based Approach in Data Protection Legal Frameworks' (n 20) 4.

[26] Daran Hallinan and Nicholas Martin, 'Fundamental Rights, the Normative Keystone of DPIA' (2020) 2020 European Data Protection Law Review 178.

[27] Article 1(2) GDPR.

[28] Niels van Dijk, Raphaël Gellert and Kjetil Rommetveit, 'A Risk to a Right? Beyond Data Protection Risk Assessments' (2016) 32 Computer Law & Security Review 286, 289.

[29] Raphaël Gellert, *The Risk-Based Approach to Data Protection* (Oxford University Press 2020) 26–42.

[30] ibid., 30-31.

deemed necessary, the assessment should also provide for risk mitigation measures to help reduce risks to an acceptable level.[31] Risk management methods pretend to objectivity. As Gellert explains, "risk analysis", a prominent risk management method, is based on quantitative risk assessment grounded in natural sciences.[32] The pretense in objectivity has been criticised by literature, which considers risks to be both factual and value statements.[33] Deciding on the risk criteria, which risk to prioritise, and which risk is worth taking presupposes certain value judgments. The fact remains though that risks are commonly defined through scientific concepts of probability.[34]

Fundamental rights, on the other hand, traditionally have had a different function. They are not a tangible concept which can be scientifically quantified. Rather, they may best be described as "abstract social concepts" and "intangible moral values" linked to human dignity, aimed to protect against mainly intangible harms.[35] The legal protection fundamental rights afford stems from national constitutions and international human rights instruments, and is typically shaped through jurisprudence *after* an alleged breach has taken place. It is through case law that the vague right to "private life", for instance, has been and is still being elucidated. Fundamental rights protection is thus to a large extent reactive, even though the obligation of states to respect fundamental rights and the possibility of legal challenges has meant that fundamental rights are taken into consideration also in the adoption of laws and policies by state actors.

In light of the above, van Dijk et al. have demonstrated how by placing "risks" and "fundamental rights" together, data protection law changes the understanding and practice of both concepts.[36] One the one hand, because fundamental rights are now the object of the risk assessment, identifying and assessing risks cannot only be a matter of natural science, statistics and probabilities. And on the other hand, given the anticipatory and uncertain nature of risks, fundamental rights protection becomes anticipatory instead of reactive, and is no longer the task of courts and legislators: individual data controllers now need to identify, assess and mitigate risks to rights.

---

[31] ibid.

[32] ibid., 37.

[33] Ulrich Beck, 'Risk Society Revisited: Theory, Politiques, Critiques and Research Programmes' in Barbara Adam, Ulrich Beck and Joost van Loon (eds), *The Risk Society and Beyond: Critical Issues for Social Theory* (SAGE 2012) 138.

[34] van Dijk, Gellert and Rommetveit (n 28) 289.

[35] Yeung and Bygrave (n 14) 7.

[36] van Dijk, Gellert and Rommetveit (n 28) 289.

1.3 The accountability principle and the ensuing "decentralisation"

1.3.1 The nexus between accountability and risk

ACCOUNTABILITY AS A META-PRINCIPLE. The principle of accountability is to be found in article 5(2) GDPR, which states that "the controller shall be responsible for, and demonstrate compliance with" the principles for processing of personal data of Article 5(1). It is thus not sufficient that the processing complies with GDPR obligations; this compliance should also be *demonstrated.* The requirement to demonstrate compliance was implemented following the recurring problems of poor compliance and data losses stemming from the previous reactive approach to data protection.[37] The questions arise, however, how to demonstrate accountability. Urquhart and Chen argue that Article 5(2) should be read broadly as also requiring compliance with Article 24 GDPR on the responsibility of controllers, and even the entire GDPR; they state that accountability in the GDPR is a meta-principle that provides guidelines on how other principles should be observed.[38] From this perspective, then, to demonstrate accountability, controller has to implement "appropriate technical and organizational measures,"[39] which inevitably ties accountability with risk assessment and requires controllers to take procedural steps towards demonstrating accountability.[40] There is thus a close link between the notion of risk and the notion of accountability, because risk control is materialising through [a] new enforced self-regulation model.[41]

ANTECEDENTS. Accountability of data controller that materializes through their obligation to demonstrate compliance with data processing principles can be traced in other legal instruments than the GDPR. The 2013 OECD Guidelines, requiring openness and enabling right of individuals, which formulate accountability compliance in the sense of what *individuals* can "do, ask and challenge" by the data controller.[42] In turn, WP29 does not formulate

---

[37] Katerina Demetzou, 'Data Protection Impact Assessment: A Tool for Accountability and the Unclarified Concept of "High Risk" in the General Data Protection Regulation' (2019) 35 Computer Law & Security Review 105342, 14.

[38] Lachlan Urquhart and Jiahong Chen, 'On the Principle of Accountability: Challenges for Smart Homes & Cybersecurity' (2020) Paper available at SSRN 4.

[39] Art. 24(1) GDPR.

[40] See, Raphaël Gellert, 'Understanding the Notion of Risk in the General Data Protection Regulation' (2018) 34 Computer Law & Security Review 279, 280 – 281; Katerina Demetzou (2019) GDPR and the Concept of Risk: The Role of Risk, the Scope of Risk and the Technology Involved, in: Kosta E., Pierson J., Slamanig D., Fischer-Hübner S., Krenn S. (eds) Privacy and Identity Management. Fairness, Accountability, and Transparency in the Age of Big Data. Privacy and Identity 2018. IFIP Advances in Information and Communication Technology, vol 547. Springer, Cham, 143.

[41] Macenaite (n 18) 524.

[42] OECD Guidelines on the Protection of privacy and transborder flows of personal data (1980, revised in 2013) available at https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf, p 23.

accountability in concrete actions, nor is it entirely clear who is the "acountée." According to WP29, such approach (while indeed leaves the decision on how, when and by which means to prove accountability to controller) is necessary to enable flexibility.[43] When comparing the approach of OECD and the GDPR/WP29, Urquhart and Chen argue that since OECD does not require demonstration of accountability, its framing of accountability is broader than the one of the EU.[44]

1.3.2 Accountability mechanisms in the GDPR: the DPIA as "meta-regulation"

The principle of accountability, and its grounding in a risk-based approach, culminates with the obligation for controllers to conduct a DPIA when a processing operation is likely to result in a high risk to the rights and freedoms of natural persons.

DPIA CONTENT. The DPIA is the main exercise meant to identify and address the risks of a processing operation to the rights and freedoms of individuals. Its core in provided in Article 35(7) GDPR, according to which the assessment must contain at least: a) a systematic description of the envisaged processing operations, their purposes and interests pursued; b) an assessment of the necessity and proportionality of the processing operations in relation to the stated purposes; c) an assessment of the risks to the rights and freedoms of data subjects; d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the GDPR, taking into account the rights and legitimate interests of data subjects and other persons concerned.

DPIA AS META-REGULATION. The obligation to conduct a DPIA has been characterized as one of the GDPR's most significant forms of meta-regulation.[45] Because DPIAs are conducted by the regulated entities (i.e., controllers), and are meant to address the risks arising from the controllers' behaviour, they constitute a move towards self-assessment. Just as meta-regulation strategies prescribe, they call on controllers to take responsibility for assessing and mitigating risks themselves.[46] This approach could significantly enhance the effectiveness of the data protection regime, because it leverages the controllers' ability to manage themselves, and cultivates within them a culture in which data protection and risks to rights are taken seriously.[47]

---

[43] Article 29 Data Protection Working Party 'Opinion 3/2010 on the Principle of Accountability' p 14.

[44] Urquhart and Chen (n 38).

[45] Binns (n 7); Yeung and Bygrave (n 14) 6.

[46] Yeung and Bygrave (n 14) 6.

[47] ibid.

EFFECTIVE META-REGULATION? Meta-regulation strategies have been employed, prior to data protection, in other sectors.[48] From these other experiences it is possible to identify not only benefits of meta-regulation, but also drawbacks, which could serve as food for thought on possible pitfalls of the GDPR's focus on accountability, risks and the DPIA. According to the literature, to be effective, meta-regulation requires that in addition to the regulated organisations, regulators themselves and external stakeholders must have a role in a "triple loop" of evaluation.[49] Studies have indeed demonstrated that independent scrutiny is important, because the regulated organisations, left entirely by themselves, may fail to conduct proper self-assessments.[50] Such failures may not only intentional but also result from lack of knowledge, especially where an assessment pertains to complex matters.

1.4 Conclusion: Significant powers granted on controllers

The key positioning of accountability and risk in the GDPR constitutes a shift from centralized to more decentralized regulation with the accountability of data controllers at its core.[51] Because the GDPR operates on the basis of open norms (the principles) and the equally broad notion of risk, controllers have important decision-making powers: to identify and assess risks, to reflect on desired outcomes and measures that should be taken to ensure compliance with data protection principles and, overall, to ensure a fair balancing of their interests and the interests of individuals who are subject to the processing. Their responsibility requires them to deal with legal, qualitative and substantive issues of legitimacy, fairness and proportionality. Under this regulatory framework, controllers may no longer be ascribed the role of mere subjects of data protection law, as they become active decision-makers.[52]

While such a decentralized and risk-based framework has important benefits in view of the need for a flexible and future-proof legal framework to regulate data processing, it is not without risks. Ultimately, too much depends on the controllers' willingness and ability to properly interpret and fulfil their responsibilities. The complexity of the concept of "risks to rights and freedoms" makes exercises such as the DPIA bewildering ones,[53] especially in the absence of

[48] Binns (n 7) 30.

[49] Christine Parker, *The Open Corporation: Effective Self-Regulation and Democracy* (Cambridge University Press 2002) 246–248.

[50] Binns (n 7) 31.

[51] Damian Clifford and Jef Ausloos, 'Data Protection and the Role of Fairness' (2018) 37 Yearbook of European Law 130, 182–183.

[52] Claudia Quelle, 'Enhancing Compliance under the General Data Protection Regulation: The Risky Upshot of the Accountability- and Risk-Based Approach' (2018) 9 European Journal of Risk Regulation 502, 526.

[53] Yeung and Bygrave (n 14) 6.

concrete guidelines. There is thus a clear threat that accountability is viewed as a box-ticking exercise,[54] with controllers favouring documentation and compliance with processes, instead of aiming to achieve the substantive the GDPR's to protect fundamental rights which may be at risk by the processing.

To avoid this danger, evaluation and monitoring of controllers' behaviour –broadly referred to in this Deliverable as "enforcement"- is crucial. It is thus necessary to examine in the next session the enforcement mechanisms foreseen in the GDPR and discuss the extent to which they are able to ensure effective protection of citizens' rights which may be endangered by a processing operation.

[54] ibid.

2 ENFORCEMENT MECHANISMS UNDER GDPR'S DECENTRALIZED MODEL: OPPORTUNITIES AND CHALLENGES

2.1 Data Protection Authorities

BROAD TASKS AND POWERS. Independent supervisory authorities have a fundamental role in the EU data protection legal framework. The provision in Article 8(3) CFR, an instrument of primary EU law, according to which compliance with data protection rules shall be subject to control by an independent authority attests to their importance. Articles 57 and 58 GDPR vest Data Protection Authorities (DPAs) with numerous tasks and the necessary investigatory, corrective and advisory powers to exercise such tasks. To illustrate the breadth of their functions, it is worth mentioning that Article 57 stipulates 22 tasks, which essentially give DPAs "the roles of ombudsmen, auditors, consultants, educators, policy advisors, negotiators and enforcers".[55] Two are particularly pertinent to stress for the purposes of this Deliverable on decentralised regulation and enforcement: the advisory role and the role of enforcer.

ADVISORY ROLE. The GDPR foresees that national DPAs shall promote "public awareness and understanding of the risks, rules, safeguards and rights in relation to [the] processing [of personal data]"[56], as well as "the awareness of controllers and processors of their obligations under [the] Regulation".[57] The European Data Protection Board (EDPB), comprising of representatives of national DPAs, can also issue opinions and guidelines following the practice of its predecessor WP29.[58] Such European guidelines should enable the consistent interpretation of GDPR's legal provisions throughout the EU.

Because the GDPR is a principle-based regulation, the advisory role of DPAs is particularly important. The opinions and guidelines they issue help shed clarity over broad and vague notions in the Regulation, such as purpose limitation or legitimate interests. For instance, the WP29 Guidelines on DPIAs have provided certain criteria that are meant to guide controllers in determining whether a processing operation is likely to result in a high risk to the rights and freedoms of

[55] Hielke Hijmans, 'Article 57. Tasks' in Christopher Kuner, Lee A Bygrave and Christopher Docksey (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020) 993, referring to the work of Colin Bennett and Charles Raab, *The Governance of Privacy* (Ashgate Publishing) 109–114.

[56] Article 57(1)(b) GDPR.

[57] Article 57(1)(d) GDPR.

[58] Article 70(1) on the tasks of the EDPB.

individuals.[59] The advisory role enables DPAs to issue soft law instruments that offer more legal certainty to controllers, by guiding them on how to interpret provisions and achieve compliance with GDPR's often vague legal requirements.[60]

ENFORCER. DPAs are also tasked to monitor and enforce the application of the Regulation.[61] To this end, the GDPR has granted them extensive investigative powers, including the power to order controllers and processors to provide any information a DPA needs to perform its tasks; to carry out data protection audits; to obtain access to premises of controllers and processors, and to all data and information necessary in the course of an investigation.[62] In case of possible violations, DPAs have corrective powers such as the power to issue warnings, reprimands, and even administrative fines to controllers and processors.[63]

FROM EX-ANTE TO EX-POST ENFORCEMENT. Importantly, under the GDPR, monitoring and enforcement by DPIAs to a large extent happen after a processing operation has started. While Directive 95/46/EC (Data Protection Directive) had certain mechanisms for the "prior checking" of controllers' operations, the GDPR no longer follows that approach. To explain, the Data Protection Directive required controllers to notify personal data processing to DPAs in order to ensure that the purposes and main features of such processing were public and open for DPAs to verify.[64] For operations likely to present specific risks to the rights and freedoms of data subjects, the Directive provided that they should be examined and checked by DPAs before they start taking place.[65]

The GDPR has replaced this ex ante notification and prior checking monitoring mechanisms that involved the DPAs, with accountability obligations such as the appointment of Data Protection Officers (DPOs) and the conduct of DPIAs in cases of high risk processing, which are to be carried out by controllers. The only monitoring mechanism that involves the DPA ex ante is the one provided in Article 36 GDPR. The provision requires controllers to launch a formal prior consultation procedure with the DPA in case they have completed a DPIA, yet despite such DPIA they are not able to take measures to mitigate risks to an acceptable level: in other

[59] Article 29 Data Protection Working Party, 'Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing Is "Likely to Result in a High Risk" for the Purposes of Regulation 2016/679' (2017) WP 248 rev.01.

Christofi and others (n 4) 146.

[61] Article 57(1)(a) GDPR.

[62] Article 58(1) GDPR.

[63] Article 58(2) GDPR.

[64] Article 18 Directive 95/46/EC (no longer in force). The Directive enabled Member States to introduce certain simplifications or exceptions to the notification requirement for low risk processing operations.

[65] Article 20 Directive 95/46/EC (no longer in force).

words, where unacceptable residual risks remain.[66] The DPA should then communicate its written advice to the controller where it considers that the intended processing would infringe the GDPR.[67]

RISK AND ENFORCEMENT. Analysing DPIAs as an expression of meta-regulation, Binns has pointedly argued that the success of a meta-regulatory approach to DPIAs "will significantly depend on the capacity of supervisory authorities to independently scrutinize data controller's proposed mitigation strategies".[68] The same is arguably true for the success of the GDPR as a regulation which favours principles, a risk-based approach, accountability and decentralization. Monitoring and enforcement by DPAs is much needed, yet how could it be effectively exercised in practice in an era of countless controllers and processing operations? A risk-based approach is in fact recommended also as regards enforcement by DPAs.[69] According to the WP29, the role of DPAs with respect to the risk-based approach established by the Regulation consists inter alia of "targeting compliance action and enforcement activity on areas of greatest risk". [70]

2.2 Control by data subjects

DATA SUBJECTS MONITORING CONTROLLERS. Aside from DPAs, the GDPR provides for mechanisms and tools that enable data subjects themselves to monitor the behaviour of controllers and compliance with the Regulation. A first mechanism are the data subject rights recognised in the GDPR, and in particular the provisions linked to transparency and information (Arts. 12-14) and the right of access (Art. 15). The exercise of such rights requires controllers to provide information about the purposes of processing, the types of personal data involved, the data retention period, possible data recipients, and even copies of the personal data undergoing processing. This information arguably enables data subjects to exercise some form of scrutiny over controllers' practices. Even though there are certainly challenges in the ability of data subjects to effectively contribute to the enforcement of the GDPR, the importance of these rights for enforcement should not be underrated. The *Schrems* judgment,[71] which started from a complaint to the Irish DPA against Facebook and led to the annulment of

[66] Cecilia Alvarez Rigaudias and Alessandro Spina, 'Article 36. Prior Consultation' in Christopher Kuner, Lee A Bygrave and Christopher Docksey (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (2020) 683–685.

[67] Article 36(2) GDPR.

[68] Binns (n 7) 32.

[69] Quelle (n 52) 510.

[70] Article 29 Data Protection Working Party, 'Statement on the Role of a Risk-Based Approach in Data Protection Legal Frameworks' (n 20) 4.

[71] Case C-362/14, Maximillian Schrems v Data Protection Commissioner ECLI:EU:C:2015:650

the Commission Decision that legitimized data transfers from the EU to the United States, began with the exercise by Schrems of his right of access vis-à-vis Facebook.

COMPLAINTS AND REMEDIES. Linked to the above are the remedies that the Regulation provides for data subjects. Notably, data subjects have the right to lodge a complaint with the competent DPA if they consider that a processing operation involving their personal data infringes the GDPR.[72] A right to an effective judicial remedy is also enshrined. It is possible to seek a judicial remedy against the DPA, where the DPA does not handle a complaint, or dismisses it partially or entirely.[73] Bringing court proceedings against controllers or processors is also possible where data subjects believe there has been a violation of the Regulation.[74] Finally, any person who has suffered material or non-material damage due to an infringement of the GDPR has the right to receive compensation for the suffered damage from the responsible controller or processor.[75]

DATA SUBJECTS REPRESENTATION. The GDPR therefore gives, at least in theory, rights and remedies that allow data subjects to detect possible infringements and hold controllers accountable. Yet, these mechanisms can be meaningless if data subjects lack the knowledge and means (e.g. financial) to pursue them. The challenge has been well-illustrated in a report the EU Fundamental Rights Agency (FRA) published in 2013,[76] ahead of the GDPR's adoption. As Fuster explains, the report suggested that there is a persistent lack of knowledge on data protection not only among data subjects, but also across the judiciary.[77] The effectiveness of the available redress mechanisms is hampered by such lack of expertise. To address this problem, according to FRA, the role of specialized NGOs should be strengthened by providing them with more resources and funding, and importantly by relaxing the rules on legal standing so that they are also able to lodge data protection-related complaints.[78]

---

[72] Article 77 GDPR.

[73] Article 78 GDPR. See also: Waltraut Kotschy, 'Article 78. Right to an Effective Judicial Remedy against a Supervisory Authority' in Christopher Kuner, Lee A Bygrave and Christopher Docksey (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020) 1130.

[74] Article 79 GDPR.

[75] Article 82 GDPR.

[76] European Union Agency for Fundamental Rights, 'Access to Data Protection Remedies in EU Member States' (2013).

[77] Gloria González Fuster, 'Article 80. Representation of Data Subjects' in Christopher Kuner, Lee A Bygrave and Christopher Docksey (eds), *The General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020) 1143.

[78] ibid., 1143-1144.

The issue of representation has been addressed by the Regulation. Article 80 provides a right to representation, aimed "to strengthen and facilitate the defence of the interests of data subjects". The entities that can be mandated to represent data subjects must: be not-for-profit bodies, organisations or associations (1); be properly constituted under the law of a Member State (2); have public interest related statutory objectives (3); be active in the data protection field (4). If these conditions are fulfilled, these entities can represent data subjects both when lodging a complaint with the DPA, or when seeking a judicial remedy against DPAs and/or against controllers or processors.

Article 80 then gives the option for Member States to enable such entities to file complaints with the DPA and court proceedings irrespective of a data subject's mandate.[79] In other words, to seek to protect the right to data protection and to enforce data protection law on their own initiative, even where no specific data subject has mandated them to do so. The right of NGOs for non-mandated actions is not a generally applicable one, as it depends on Member States' willingness to enshrine it in their national law. In Belgium, although the national law implementing the GDPR does not mention the possibility of non-mandated actions, the possibility arguably exists in view of other legislation.[80]

2.3 Codes of conduct and certification

RATIONALE. To facilitate its effective application, the GDPR also provides for co-regulatory instruments, notably codes of conducts[81] and certification mechanisms.[82] Co-regulation is a regulatory "model that combines both legislation and self-regulatory instruments in support of the law".[83] In line with this approach, the GDPR entrusts certain regulatory functions to associations representing different sectors or to certification bodies with an appropriate expertise in relation to data protection. While adherence to these mechanisms is voluntary, there are three main arguments in support of codes of conduct and certification mechanisms. Firstly, they assist controllers and processors to comply and (in line with the accountability principle) to demonstrate their compliance with the GDPR. Codes of conduct, for instance, do so by focusing on the characteristics and risks of processing in *specific* sectors, calibrating the GDPR's

[79] Article 80(2) GDPR.

[80] Notably, the Law of 28 March 2014, which enables representative entities to start actions on behalf of victims without obtaining any previous mandate. See: Alexia Pato, 'The Collective Private Enforcement of Data Protection Rights in the EU' (2019) Paper available at SSRN.

[81] Article 40 GDPR.

[82] Article 42 GDPR.

[83] Irene Kamara, 'Co-Regulation in EU Personal Data Protection: The Case of Technical Standards and the Privacy by Design Standardisation "Mandate"' (2017) 8 European Journal of Law and Technology 2 <https://ejlt.org/index.php/ejlt/article/view/545> accessed 4 June 2021.

legal obligations to the level of risk relevant to each sector.[84] Certification mechanisms can be a means to demonstrate compliance with specific GDPR obligations such as security and data protection by design and by default.[85] Secondly, they assist DPAs in their supervisory functions, as adherence to codes of conduct and certification mechanisms is monitored by independent bodies.[86] Thirdly, they provide transparency to data subjects and to the market more broadly (e.g. private and public authorities wishing to purchase a software) as they allow one to quickly assess whether a product or service has an adequate level of protection.[87] Thus, although adherence to a code of conduct and/or a certification mechanism is voluntary for controllers and processors, it comes with an important advantage.

OPPORTUNITIES YET SLOW DEVELOPMENT. Codes of conduct and certification mechanisms essentially give the power to private entities (e.g. industry associations, certification bodies) to specify and monitor GDPR compliance. This co-regulatory framework was nevertheless crafted to ensure that the ensuing private and voluntary rules are consistent with the GDPR's public values and principles, and do not pursue a de-regulatory agenda.[88] Two factors in the design of these mechanisms support this argument. First, public regulators, notably the EDPB and national DPAs are closely involved in the adoption of these mechanisms. As regards certification, they approve the certification criteria and the requirements for the accreditation of certification bodies.[89] They also have the power to sanction or revoke accreditation in case these bodies fail to comply with their accreditation mandate.[90] Codes of conduct also need to be approved by DPAs.[91] Secondly, the GDPR requires such mechanisms to operate in a transparent manner. For instance, certification must "be voluntary and available via a process that is transparent";[92] and the procedures and structures to handle complaints foreseen in the codes of conduct and certification mechanisms have to be transparent to data subjects and the public.[93]

---

[84] Irene Kamara, 'Article 40. Codes of Conduct' in Christopher Kuner, Lee A Bygrave and Christopher Docksey (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020) 718.

[85] Ronald Leenes, 'Article 42. Certification' in Christopher Kuner, Lee A Bygrave and Christopher Docksey (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020) 738.

[86] Kamara (n 84) 718.

[87] Leenes (n 85) 733.

[88] Christofi and others (n 4).

[89] Article 51(1) (n) and (p) GDPR.

[90] Article 43(7) GDPR.

[91] Article 40(5) GDPR

[92] Article 42(3) GDPR.

[93] Articles 41(2)(c) and 43(2)(d) GDPR.

.

This co-regulatory nature of codes of conduct and certification mechanisms arguably makes their development slower, compared to for instance completely self-regulatory mechanisms like standards developed by ISO.[94] Their development is also seemingly resource intensive. Industry associations have argued that developing codes of conduct entails a significant organizational and financial burden for the industry association,[95] and that the emergence of national codes of conducts risks fragmenting the development of a European market for the specific sector.[96]

2.4 Weaknesses of current enforcement mechanisms

Under the GDPR's principle- and risk-based approach, decisions on data protection issues mainly rely on controllers. Scrutiny over controllers' decisions is thus crucial for ensuring effective application and enforcement. This section presents the main criticisms to this approach.

2.4.1 Reliance on controllers and limited resources for their supervision

CONTROLLERS IN A CONFLICT OF INTEREST? Analysing the "legitimate interests" legal basis in Article 6(1)(f), which requires controllers to balance their interests with the rights and interests of the data subjects, Ferretti noted how controllers "would be in a position of clear conflict of interest" when conducting this balancing themselves. Arguably, this concern goes beyond that specific provision to the many instances and provisions in the GDPR where controllers need to engage in some form of interpretation and application of broad, vague principles. Because it is often in their interest to process (many) data, they may opt for interpretations that favour their interests.

COMPLEXITY OF DATA PROTECTION LAW. In his thought-provoking piece "The trouble with European data protection law", Koops argued that one of that law's main fallacies is the "too much faith" it places in controllers' actions.[97] He explained that

[94] Christofi and others (n 4).

[95] Insurance Europe, 'Response to the EDPB's Draft-Guidelines on Codes of Conduct & Monitoring Bodies, Position Paper Referring to Guidelines 1/2009 on Codes of Conduct & Monitoring Bodies under Regulation 20116/679' (4 October 2019) <https://www.insuranceeurope.eu/sites/default/files/attachments/Response%20to%20EDPB%20draft-guidelines%20on%20codes%20of%20conduct%20%26%20monitoring%20bodies.pdf>.

[96] DIGITALEUROPE, 'Response to Public Consultation on Draft EDPB Guidelines on Codes of Conduct and Monitoring Bodies' (4 May 2019) <https://www.digitaleurope.org/resources/response-to-public-consultation-on-draft-edpb-guidelines-on-codes-of-conduct-and-monitoring-bodies/>.

[97] Bert-Jaap Koops, 'The Trouble with European Data Protection Law' (2014) 4 International Data Privacy Law 250, 253.

even though controllers may be well-intentioned and want to comply, the complexity of data protection with the open-ended language used in key definitions and requirements make compliance difficult in practice. Ex ante obligations like mandatory DPIAs might be useful, but it is doubtful whether these processes will be used by controllers to seriously think about data processing's risks to fundamental rights and how they can be minimized, or will rather function as paper checklists, with controllers considering that because the procedure has been followed problems have been solved.[98]

Similarly, Yeung and Bygrave explained why undertaking a GDPR-compliant DPIA which addresses risks to fundamental rights and freedoms can be a particularly difficult exercise for controllers.[99] The main reason is the conceptual difficulty surrounding fundamental rights. Because these rights entail intangible moral values and rest on conceptual abstractions, they are difficult to comprehend and apply by entities –in casu, controllers- who are not well familiar with fundamental rights law and practice. DPIAs require controllers to not only consider the data subject rights recognised in the GDPR (e.g. information, access, erasure), but fundamental rights more generally. Given that such rights are state-centric obligations (since they primarily place obligations on states and state actors), extensive knowledge and experience are unlikely to be found in private organisations.[100]

This makes guidance on how to undertake a DPIA which assess risks to rights crucial. Yet, whether it already exists in DPIA guidelines is doubtful. WP29 Guidelines on DPIAs focus on providing criteria indicating that a processing operation may be "high risk" but leave the issue of possible consequences of such risk on fundamental rights and how they can be avoided vague.[101] Instead, they refer to assessment methodologies that embrace a more quantitative and information security approach, such as ISO/IEC 2913434 Privacy Impact Assessment Guidelines. The latter follow a narrower understanding of risks, which focuses on information security management systems, and attempt to quantify them. They are thus not fully aligned with how the GDPR views the DPIA as an exercise that considers and addresses risks to fundamental rights.[102]

DPA MONITORING. In light of the above, both the advisory and supervisory functions of Data Protection Authorities are crucial. The extent to which they can

[98] ibid., 253-255.

[99] Yeung and Bygrave (n 14) 11.

[100] ibid.

[101] ibid.

[102] For an analysis of the 'misalignment' between DPIAs as foreseen under the GDPR on the one hand, and the ISO/IEC Guidelines on the other hand see: Christofi and others (n 4).

effectively fulfil the wide-ranging and important roles assigned to them by the GDPR nevertheless depends on their resources. Resources are provided by the Member States, and can thus widely vary from one State to another. Authors have noted how traditionally, DPA resources have been scarce in most States,[103] which casts real doubt on the authorities' ability "to provide effective oversight over a myriad of data controllers". [104] Even if a risk-based approach is taken with regard to enforcement, whereby DPAs are called to prioritise risky sectors and processing operations, there may simply be too many of these operations in an era of ubiquitous and constantly developing processing technologies.

2.4.2 Data subjects and their representatives can in practice exercise limited oversight

2.4.2.1 A. Consent, data subjects rights and the limits of such classic control tools

LIMITS OF DATA SUBJECTS CONTROL. Giving individuals greater control over the processing of their personal data has often been portrayed as the solution to the challenges data processing technologies raise.[105] In the GDPR, efforts have been made to strengthen the requirements for consent and the data subjects rights. Consent and these rights embody an individualistic understanding of control, which emphasises individual choice and self-management when it comes to data processing. This emphasis on individual control has been viewed critically by scholarship. Lazaro and Le Metayer have argued that individuals' capacity to self-manage their privacy and personal data is compromised by factors such as incomplete information, bounded rationality, and systematic psychological deviations from rationality.[106] The latter two denote the challenges, for humans, to compute all relevant information and calculate the gains and losses linked to each decision, and take rational decisions. The authors observe how individuals may pass their personal data in exchange for very small benefits or rewards because it is difficult to assess the trade-offs between such immediate gains (albeit small) and more speculative long-term risks and benefits. Similar concerns have been voiced by Cohen, noting that even when disclosures about data processing are truthful, data subjects may be induced to consent and to over-disclose personal information.[107]

[103] Yeung and Bygrave (n 14) 13.

[104] Koops (n 97) 255.

[105] Christophe Lazaro and Daniel Le Métayer, 'Control over Personal Data: True Remedy or Fairy Tale?' (2015) 12 SCRIPTed 3, 4.

[106] ibid., 10-12.

[107] Julie E Cohen, 'Turning Privacy Inside Out' (2019) 20 Theoretical Inquiries in Law 7 <https://www7.tau.ac.il/ojs/index.php/til/article/view/1607> accessed 7 June 2021.

2.4.2.2 *Participation In DPIAs: the opportunity and challenges of Article 35(9) GDPR*

INABILITY TO SHAPE THE DESIGN OF PROCESSING. Data subjects' literacy and decisions over disclosures of their personal data can be improved over time as knowledge of the risks of data processing and of data protection rights increase. Yet, the fact remains that in its current form the GDPR entrusts controllers with important decisions on the processing, only recognising the possibility for -rather than clearly mandating- the involvement of data subjects in such decision-making. These are notably decisions about the necessity, proportionality and design of a processing operation, the risks it poses to the rights and freedoms of individuals and how they can be mitigated, which are all matters that should be addressed in the DPIA process.

PARTICIPATION IN DPIAS – ART. 35(9) GDPR. Some form of participation of data subjects and/or their representatives in DPIAs is foreseen in Article 35(9) GDPR. According to the provision:

"Where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations."

OPPORTUNITIES. Involving data subjects or their representatives in DPIAs, as provided in Article 35(9) GDPR, may have important advantages. As explained above, data subjects rights are mostly triggered ex post facto, and their exercise is individualistic: one has the right to access or rectify his or her own personal data. Article 35(9) enables ex ante involvement and the participation of individuals in the risk identification and assessment exercise, where they can provide views on how the processing could impact fundamental rights and freedoms more broadly. The quality of the DPIA, which is a key accountability instrument under the GDPR, is improved because there is a multi-perspective exploration of the risks of a processing operations.[108] The input of data subjects or their representatives can be particularly beneficial for controllers, since knowing the concerns of individuals at an early stage gives them the opportunity to address such concerns, and to potentially avoid complaints to DPAs or courts once the processing starts taking place. There can also exist benefits for the data subjects

[108] Anthony Morton and others, '"Tool Clinics" – Embracing Multiple Perspectives in Privacy Research and Privacy-Sensitive Design' in Alessandro Acquisti and others (eds), *My Life, Shared - Trust and Privacy in the Age of Ubiquitous Experience Sharing* (Dagstuhl Reports 2013). The authors do not refer to DPIAs, but explain how multi-perspective exploration and problem analysis improve decision-making and increase the chances of successful technology development.

themselves. Data processing technologies may entail some risks, but also important benefits and opportunities for data subjects and society. Classic control tools in data protection law, such as consent or the data subjects rights, mainly protect individuals by shielding them from processing: if one opts to not give consent to the processing, or object to it, he or she is indeed likely not to incur any risks. At the same time, the opportunities to fully participate in a society that is increasingly digital may be limited where he or she exercises such control. The involvement of individuals in DPIAs can enable them to better understand and cope with technological changes and their risks and express their concerns, Interactions between individuals and their and controlling institutions (in casu, controllers) on the basis of mutual respect and critical reflection can foster change and evolution in the mindsets of both, and ultimately increase data subjects' trust.[109]

UNCLEAR FORMULATION. As DPIAs are a form of Impact Assessment (IA), Article 35(9) essentially provides what is commonly recognised as a best practice in IAs.[110] IAs actively involve stakeholders and consider their attitudes and expectations – in other words, they are participatory and deliberative exercises.[111] The formulation of Article 35(5) nevertheless raises important questions on the nature and the extent of a requirement to open up DPIAs to participation. "Where [is it] appropriate" to seek the views of data subjects or their representatives? Clarifying the meaning of this opening clause is crucial to understand whether there is a legal obligation to consult in the first place. If "seeking the views" is mandatory, what are the exact obligations it entails on controllers in terms of gathering and using these views? Who are the specific data subjects or their representatives that should be involved in the DPIA? And finally, wouldn't the "without prejudice" clause risk enabling controllers to invoke broad commercial or public interests as a reason not to engage with such data subjects or representatives?

DPA GUIDELINES ONLY PROVIDE LIMITED CLARITY. Even though some DPAs – including the WP29- have issued extensive guidelines on DPIAs, the guidelines fail

[109] Jo Pierson, 'Online Privacy in Social Media: A Conceptual Exploration of Empowerment and Vulnerability.' [2012] Communications & Strategies 99. While Pierson's analysis focuses on the online social media context insights are relevant for broader data processing technologies.

[110] Dariusz Kloza and others, 'Data Protection Impact Assessments in the European Union: Complementing the New Legal Framework towards a More Robust Protection of Individuals' (d.pia.lab Policy Brief No 1 2017) 2.

[111] ibid.

to exhaustively tackle the above-mentioned questions. Having consulted five of such guidelines,[112] we have observed the following:

- "Where appropriate": Guidelines fail to provide clarity on where exactly it is appropriate to seek the views of data subjects or their representatives in the DPIA. Rather, they clarify that this is a decision for controllers to make,[113] in line with the accountability principle. WP29 DPIA Guidelines, for instance, only require controllers to "document" the reasons why they consider consultation not to be appropriate.[114] Some guidelines do note that the obligation in Article 35(9) "is not entirely optional" because the nature, context, scope and purpose of the processing as well as its potential impact on the persons concerned may render consultation mandatory.[115] But since they do not further clarify which are these contexts, purposes and impacts that would mandate involving data subjects, controllers still enjoy significant discretion in their decision to involve or not.

- "Seek the views": It is clear from the guidelines, but also the formulation of Article 35(9) that views must be sought, which entails that an actual consultation must take place.[116] The mere provision of information on the processing to the affected data subjects would thus not meet the requirements of the provision. How to gather the views depends on the context. Examples mentioned include generic studies, questions and surveys.[117] Some guidelines recommend creating a consultation strategy and process.[118]

---

[112] Notably: WP29, 'Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is 'likely to result in a high risk' for the purposes of Regulation 2016/679' (2017) wp248rev.01 (EU-wide); ICO, 'Data Protection Impact Assessments (DPIAs)' (2018) (United Kingdom); Data Protection Commission, 'Guide to Data Protection Impact Assessments (DPIAs)' (2019) (Ireland); CNIL, 'Privacy Impact Assessment (PIA) Methodology' (2019) (France); Commission de la Protection de la Vie privée (CPVP), 'Recommandation d'initiative concernant l'analyse d'impact relative à la protection des données et la consultation préalable (CO-AR-2018-001)' (2018) (Belgium).

113 E.g. the CPVP o.c. para. 82 explains that 'the decision whether or not to consult is first and foremost the responsibility of
the controller'. ICO o.c. 33 states '[controllers] should seek and document the views of individuals (or their representatives)
unless there is good reason not to', which is to be ascertained by the controller itself.

[114] Article 29 Data Protection Working Party, 'Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing Is "Likely to Result in a High Risk" for the Purposes of Regulation 2016/679' (n 59) 15.

[115] CPVP o.c. para. 82.

[116] Article 29 Data Protection Working Party, 'Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing Is "Likely to Result in a High Risk" for the Purposes of Regulation 2016/679' (n 59) 15.

[117] ibid.

[118] ICO o.c. 33; CPVP o.c. para. 84.

Although an active consultation should take place, its findings and outcome are not binding for controllers. Guidelines explain that controllers are entitled to not follow the views of data subjects or their representatives, as long as they document the reasons for doing so.[119]

- "Data subjects or their representatives": Who are the data subjects or their representatives to be consulted is also context-specific and depends on who is possibly affected by a data processing operation. This could include future customers or the staff of a company, or even staff representatives.[120] In cases where it is impossible or challenging to identify in advance the affected data subjects or their representatives, some guidelines note that controllers could design and implement a public consultation process.[121]

- "Without prejudice": The wording of Article 35(9) GDPR suggests that commercial, public and security interests may be invoked by controller as reasons not to undertake a consultation, or limit its scope and the information provided through it. These interests are not further defined in the Regulation, nor do the guidelines invite controllers to interpret them strictly.

A PROVISION THAT IS DE FACTO IGNORED? Despite its potential to improve the quality of DPIAs and allow for some form of ex ante scrutiny over controllers' important decisions on matters of necessity, proportionality and risks, Article 35(9) risks to be an inoperative provision Controllers may have little incentives to undertake a consultation, especially taking into account the possible costs and efforts entailed. As long as the nature of the obligation contained therein is not further specified, and controllers are left with no guidelines on how to effectively gather and consider useful input from data subjects, it may be easier for controllers to argue that consultation is not appropriate, thereby bypassing Article 35(9).

2.4.2.3 Unavailability of DPIAs to the general public

NO MANDATORY PUBLICATION. The proper assessment and mitigation of the risks of a processing operation by the controller is crucial for the effective application of the GDPR in view of the importance the Regulation gives on accountability, the risk-based approach, and the need to protect the rights and

[119] Article 29 Data Protection Working Party, 'Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing Is "Likely to Result in a High Risk" for the Purposes of Regulation 2016/679' (n 59) 15.

[120] ibid.

[121] ICO o.c. 33; CPVP o.c. para. 84.

freedoms of individuals. Yet, this information is likely to remain at the drawers or electronic files of controllers. As explained above, Article 36 GDPR only requires controllers to consult the DPA where the undertaken DPIA has revealed high risks which cannot be mitigated by appropriate measures. The general investigatory and sanctioning powers granted by the GDPR to DPAs enable them to request a DPIA, scrutiny it, and stop processing operations that fail to adequately protect against risks, but such intervention only comes ex post facto. Importantly, because the publication of DPIAs is not mandatory under the GDPR, the controllers' assessments are likely to be left unchallenged. It is unlikely that DPAs will spontaneously check a large number of DPIAs, especially considering how these authorities are called to perform significant tasks with limited resources. As long as DPIAs or DPIA summaries are not published, opportunities for civil society organisations, academics and individuals to flag possible bad practices to DPAs are essentially diminished.

3 RISKS, ACCOUNTABILITY AND ENFORCEMENT IN SMART CITIES

INTRO. Section 1 has provided an overview of key enforcement mechanisms in EU data protection law and their potential weaknesses in an era of ubiquitous data processing. Shifting the focus onto smart city-related personal data processing (hereby referred to as 'smart city processing'), this Section discusses additional challenges in applying and enforcing data protection law due to the particularities and complexity of the smart city environment. These are notably: the multitude and complexity of fundamental rights that may be at stake in smart cities, and the difficulty of assessing cumulative effects arising from multiple projects (Sect. 2.1.1); the lack of transparency and limited citizen engagement in smart cities' development, contrary to the narrative of citizen-centric smart cities (Sect. 2.1.2); the involvement of private companies and the need to ensure that the smart city technologies these companies design and sell to local authorities comply with data protection law (Sect. 2.1.3).

3.1 The complex nature of "risks to rights" in smart cities

3.1.1 Fundamental rights engaged in smart cities

RIGHT TO DATA PROTECTION. An obvious fundamental right that is often engaged in smart cities is the right to data protection enshrined in Article 8 ECFR. Since it is triggered whenever personal data is processed, with "personal data" and "processing" both being particularly broad notions, the right has a broad scope of application. At the same time, the role of the right to data protection and its object(s) of protection and relationship with other rights have not yet been clearly addressed by courts and still spark stimulating academic discussions.[122] Recently, Von Grafenstein has made a very interesting proposition to conceptualise the right as one meant to regulate and protect against risks of personal data processing against other fundamental rights.[123] The author argues that the right in Article 8 and secondary data protection law may embody certain concepts of the "precautionary principle" and the "risk-based approach". The obligation to conduct a DPIA to assess "risks to the rights and freedoms of natural persons" epitomises the important role of data protection in enabling effective protection of other rights. This role is also reflected in the wording of the GDPR itself, as

[122] A detailed analysis of Article 8 EU Charter and the case law and academic discussions surrounding its application can be found in SPECTRE Deliverable 1.1 Exploring the Essence of the Right to Data Protection and Smart Cities (2019) - A report in the framework of the SPECTRE research project. Document accessible at https://spectreproject.be/.

[123] M von Grafenstein, 'Refining the Concept of the Right to Data Protection in Article 8 ECFR – Part I' (2020) 6 European Data Protection Law Review 509.

Article 1(2) provides that the Regulation "protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data": the right to data protection is protected in particular, but not only.

THE RIGHTS OF WHOM? Both Article 1(2) GDPR (subject matter and objectives) and Article 35 (DPIA) GDPR refer to the protection of or to risks to "rights and freedoms of *natural persons*". The term "natural person" is broader than the term "data subject", which is often used in the Regulation and describes the natural person whose personal data is being processed. Referring to the DPIA obligation, some authors have noted that it "requires a broad assessment of the possible range of interferences to the fundamental rights of natural persons generally", regardless of whether or not it is their personal data that are the subject matter of the proposed data processing.[124] For smart cities, this entails that while DPIAs may start from risks to the rights of those directly affected by a smart city processing operation, because it involves their personal data, they should not stop there. They should also consider how the processing operation may affect the enjoyment of fundamental rights in the city more broadly. As will be shown below, a series of fundamental rights –of data subjects stricto sensu and of citizens more broadly- may be engaged as European cities are becoming smart.

PRIVACY. The right to respect one's private life is protected by Article 7 CFR, Article 8 ECHR and several national constitutions. Concerns about smart cities' possible impacts on privacy have been well-documented in academic literature. For instance, certain smart city technologies enable geo-surveillance, and the highly detailed spatial behavior data collected and processed impact locational and movement privacy.[125] In turn, data on the movement of individuals enable the drawing of inferences about wide aspects of their daily lives. More importantly, the smart city engages not only the freedom of individuals to be left alone in obscurity, but their freedom to self-develop. Typologies of privacy indeed recognize –under the umbrella of the freedom to self-development- intellectual, decisional, associational and behavioral privacy as facets of privacy that merit protection.[126] It is these facets, which link to the values of individual autonomy, sociability and political participation that are particularly at risk where the city uses nudging and other mechanisms to eradicate unwanted behaviors or where public spaces enable hypervisibility and anonymity can no longer be ensured.

[124] Yeung and Bygrave (n 14) 10.

[125] Rob Kitchin, 'The Ethics of Smart Cities and Urban Science' (2016) 374 Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences 20160115, 6–7.

[126] Bert-Jaap Koops and others, 'A Typology of Privacy' (2017) 38 University of Pennsylvania Journal of International Law 483.

PRIVACY FOR PUBLIC SPACES. The link between privacy and public spaces that are free from surveillance has been thoroughly explored by Galič.[127] The author explains that political activity oftentimes requires anonymity; sociality needs flexibility of use of public spaces and allowing for a certain level of disorder; autonomy entails that persons are sufficiently free to do what they want and develop themselves freely. Her analysis demonstrates how these facets of privacy are closely connected to certain attributes of public spaces. Public spaces need to be open, allow flexible uses and a certain level of disorder and dissent to enable free self-development. Those attributes of public spaces are gradually eroded by the smart city paradigm as they become securitised and constantly monitored. Galič has thus developed the concept of "privacy for public spaces", essentially denoting privacy's fundamental role in upholding the characteristics of those spaces, enabling self-development, self-expression and democratic participation.[128] As pointedly argued, "the protection of privacy serves to protect [...] aspects of public space connected to political participation and sociability" so that "one should not only think of possibilities for preserving the privateness in public space but also about preserving the publicness of public space".[129] Especially when it comes to public space, it is important to understand that interferences with privacy can lead to interferences with further fundamental rights such as the freedom of expression and the freedom of assembly.

EQUALITY RIGHTS. Title III CFR recognises a series of rights related to equality. Article 21 prohibits on any ground such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation. Ensuring equality between women and men in all areas is recognised in Article 23; the rights of the child in Article 24; and rights of the eldery to lead a life of dignity and independence and to participate in social and cultural life in Article 25. As for the ECHR, Article 14 provides that the enjoyment of the rights and freedoms set forth in the Convention must be secured without discrimination on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status. Non-discrimination provisions can also often be found in national constitutions.

BIASED DATA AND ALGORITHMS. Equality rights can be engaged in smart cities in two ways. Firstly, there is the issue of potential discriminatory effects of big data

[127] Maša Galič, 'Surveillance and Privacy in Smart Cities and Living Labls: Conceptualising Privacy for Public Space' (University of Tilburg 2019) <https://research.tilburguniversity.edu/en/publications/surveillance-and-privacy-in-smart-cities-and-living-labs-conceptu>.

[128] ibid., Chapter 7.

[129] ibid., 325.

analytics resulting for instance from biased datasets and/or algorithms. Discrimination may arise at several steps of an algorithmic process and is often unintentional.[130] For example, reliance on *biased* training data –the datasets used to enable the algorithm to learn- could pass on to the algorithm past or current prejudices. Or, seemingly objective decision criteria such as a postal code may in fact be a proxy for discrimination if an area is predominantly inhabited by certain ethnic populations, or low-income families. Biases and hitches that might lead to discrimination are often not only unintentional but also difficult to solve. Resort to historic statistics would seem to be an objective, reasonable choice for datasets used to train an algorithm. Yet, historic statistics do not occur in vacuum, and therefore their objectivity should not necessarily be taken at face value. Finch and Tene explain how the use of historical arrest statistics to target law enforcement efforts into specific neighbourhoods fails to consider the history of over-enforcement in certain minority communities.[131] The seemingly objective high crime rate of the targeted neighbourhood may in fact be exacerbated due to historical biases, now embedded in the algorithm that is used to 'objectively' predict criminality and make for effective and optimised allocation of police resources.

DIGITAL EXCLUSION. A second issue relating to the enjoyment of equality rights in smart cities is the one of exclusion. Public services increasingly become digitalized, also at the local level. With e-government one can declare and/or pay their taxes, apply for social welfare benefits or parking permits by using technological communications devices. Smart city initiatives often leverage citizens and their capacity as users of technological devices, especially smartphones, to contribute to more responsive and efficient services. Apps have been developed to enable citizens report potholes, so that city authorities can identify and repair road damage more rapidly.[132] Smart mobility, which entails the creation and use of new mobility services such as ride-sharing and multimodal transportation, also relies on urban dwellers as technology users.[133] Yet, as the enjoyment of (better and more responsive) public services becomes linked to the ownership and use of technological devices, divides within the city can be

[130] Solon Barocas and Andrew D Selbst, 'Big Data's Disparate Impact' (2016) 104 California Law Review 671. The article identifies five different steps of algorithmic decision-making: the definition of the 'target variable' and 'class labels' (i), training data (ii), feature selection (iii), proxies (iv) and masking (v). According to the authors, all five create possibilities for discrimination.

[131] Kelsey Finch and Omer Tene, 'Welcome to the Metropticon: Protecting Privacy in a Hyperconnected Town Symposium: Smart Law for Smart Cities: Regulation, Technology, and the Future of Cities' (2013) 41 Fordham Urban Law Journal 1581, 1602–1603.

[132] Ibid. Finch and Tene mention, in particular, the Street Bump app developed in the city of Boston.

[133] Sofia Ranchordás, 'Smart Mobility, Transport Poverty and the Legal Framework of Inclusive Mobility' in Michèle Finck and others (eds), *Smart Urban Mobility: Law, Regulation, and Policy* (Springer 2020) 67 <https://doi.org/10.1007/978-3-662-61920-9_4> accessed 12 March 2021.

exacerbated. The deployment of a pothole smart city system in the city of Boston already demonstrated such potential. Though successful, in that several potholes had been reported and followed-up by the relevant local authorities, the deployment showed that because low-income and/or older citizens were less likely to have had a smartphone and actively use the app, the system threatened to divert city services into wealthier and trendier neighborhoods.[134] Smart cities' potential for exclusion of certain parts of the local population makes it crucial to consider (risks to) the equality rights of minorities, the elderly, low-income, and digitally-illiterate citizens.[135]

GOOD ADMINISTRATION. Finally, the CFR recognises in Article 41 a right to good administration, which includes the rights of individuals to be heard before the adoption of individual measures affecting them adversely, and to have access to their files, and an obligation for the administration to give reasons for its decisions. Admittedly, the article mainly concerns the administrative behaviour of European Union institutions, bodies, offices and agencies.[136] Its relevance for administration at the national or even local levels should nevertheless not be underrated, especially considering that the legal systems of Member States may often set out principles linked good administration, albeit without necessarily using the term "good administration".[137] They recognize the importance of administrative discretion, understood as the empowerment of public administration, by law, "to choose from among several legal possibilities, taking into account nonjuridical criteria" in a "choice that implies balancing public and private interests".[138] Ponce explains that while traditionally, on the matter of discretion, administrative law focused on the judicial review of illegal decisions and the need to protect against arbitrariness, around Europe there has been a new viewpoint that is also concerned with the quality of decisions.[139] Accordingly, administrations should not only take legal decisions, but also good decisions, and with the appropriate reasoning to support them. This viewpoint also recognises that people want to participate in decisions that affect them, and that as a consequence, transparency, democracy and sound administration would require administrations to give reasoned answers to citizens' comments.

---

[134] Finch and Tene (n 131) 1604.

[135] Sofia Ranchordás, 'The Digitalization of Government and Digital Exclusion: Setting the Scene' (University of Groningen Faculty of Law 2020) Research Paper Series No. 30/2020.

[136] Paul Craig, 'Right to Good Administration' in Steve Peers and others (eds), *The EU Charter of Fundamental Rights: A Commentary* (Hart Publishing 2014) 1070. Craig notes that in addition to EU institutions and bodies, case law suggests that Article 41 binds Member States when they act within the scope of EU law.

[137] Juli Ponce, 'Good Administration and Administrative Procedures' (2005) 12 12 Indiana Journal of Global Legal Studies 551 (2005) <https://www.repository.law.indiana.edu/ijgls/vol12/iss2/10>.

[138] ibid., 553.

[139] ibid., 554.

These good administration principles –which may translate to rights for citizens, e.g. to access information, to ask for reasons- can be put under pressure in smart cities, because smart cities often entail some form of automation of administrative local decision-making. Decisions on building permits or welfare applications may draw from data and algorithms, while sensors and analytics spread over the cities and the cloud can be used to control traffic congestion or large crowds.[140] If policies and decisions are supported, directly or indirectly, from data and algorithms, what becomes of good administration? Decisions in smart, data-driven, cities are likely to be automated on the basis of "rule of numbers".[141] Opaque algorithms designed by private vendors may embed policy decisions that barring expertise in public administrations and citizen scrutiny could go unnoticed, unexplained and unchallenged. Administrative discretion and the duty of public authorities to give reasons for their decisions thus become challenging.

3.1.2 The challenge of identifying and assessing risks to rights in smart cities

SEVERAL RIGHTS, RISKS AND THE NEED FOR EXPERTISE. Beyond issues of (re)identification of data and data security, the previous paragraphs illustrate that several rights may be at risk by smart city initiatives. The complexity of these rights and risks has a bearing on the expertise needed for controllers –in smart cities, often the local public authorities- to properly perform their GDPR accountability obligations, and in particular the DPIA and ensuing assessment of risks to the fundamental rights and freedoms of natural persons. A multi-perspective exploration and review of technological risks is important in smart cities. Yet, as van Dijk et al. note, DPIAs currently follow a rather narrow view regarding the expertise needed to perform the DPIA exercise, focusing on expertise in information security and IT architecture.[142] Their vision for a broader view, which integrates an "ecology of expert practices" and insights from law and social sciences seems particularly pertinent to identify and assess the risks of smart cities.

IMPORTANCE OF PERCEPTIONS. In addition to the need for broad expertise, the importance of gathering the views and perceptions of the laypersons affected by smart city initiatives should be stressed. The enjoyment of fundamental rights and peoples' perceptions of technological risks can be closely linked. Such a link has been established by jurisprudence. In Digital Rights Ireland, the CJEU considered

[140] Sofia Ranchordás, 'Law and Autonomous Systems Series: Cities as Corporations? The Privatization of Cities and the Automation of Local Law' (*Oxford Business Law Blog*, 18 April 2018) <https://www.law.ox.ac.uk/business-law-blog/blog/2018/04/law-and-autonomous-systems-series-cities-corporations-privatization> accessed 12 March 2021.

[141] ibid.

[142]

a violation of the right to privacy because, among other things, the indiscriminate retention of personal data that was at stake in the case "is likely to generate *in the minds* of the persons concerned *the feeling* that their private lives are the subject of constant surveillance" [*emphasis* added]. As rights like privacy, freedom of expression or assembly or freedoms linked to the use of public space aim to protect and enable the development of one's identity, individuals' fears and perceptions may indeed thwart (their) self-development.

More knowledge is needed to understand how individuals view smart cities as a whole, and the extent to which possible negative perceptions of the smart city could amount to infringements of certain rights. Research in the city of Amsterdam suggests that citizens perceive the city's datafication with "a feeling of uncertainty and hypervisibility", with hypervisibility being "often spoken about with tinges of fear and sadness".[143] Citizens were also skeptical about the ability of anonymizing personal data in smart cities, with some even arguing that "there is always a way to go back and find who is that person even if the data is anonymized and there is no identification".[144] Whether and how citizens act on these feelings is nevertheless uncertain, even though having such knowledge is pertinent to understand risks to –and even possible violations of- fundamental rights. The issue has already been raised by Clifford with regard to emotion detection technologies used in public or semi-public spaces.[145] The author rightly wonders: What if such technologies make certain citizens act in a different manner when passing next to them? What if, when these technologies are widely deployed within the city, "they alienate the citizenry from such public or [semi-public] spaces? Would such a reality not then illustrate an interference with the right to privacy especially vis-à-vis the development of one's personality?"[146] Because to a large extent they involve the subjective perceptions of individuals, these questions are very difficult to answer through a strictly legal analysis. Participatory DPIAs that leverage Article 35(9) GDPR can nevertheless map and understand perceptions and their possible impacts on the enjoyment of rights in cities.

3.2 Aggregated effects arising from the gradual accumulation of projects

A PROJECT-SPECIFIC APPROACH. At least in Europe, "smart cities" take shape through the gradual emergence of smart city projects. Smart cities are a patchwork of

[143] Shazade Jameson, Christine Richter and Linnet Taylor, 'People's Strategies for Perceived Surveillance in Amsterdam Smart City' [2019] Urban Geography 1, 1472.

[144] ibid., 1473.

[145] Damian Clifford, 'The Legal Limits to the Monetisation of Online Emotions' (PhD Thesis, KU Leuven 2019) 251.

[146] ibid.

projects that pursue different objectives, and are often proposed and controlled by different actors. Yet even though they develop gradually and in a rather haphazard way, the previous section has illustrated that smart city initiatives can affect the enjoyment of a series of fundamental rights in cities. At the same time, one should not forget that these initiatives pursue beneficial objectives for the city and its residents and visitors, such as security, better public services, efficient mobility and transport. The tension between fundamental rights and public interest objectives is addressed in fundamental rights law by resorting to "balancing", otherwise also referred to as "proportionality". This section argues that what may be a significant challenge in terms of accountability and effective protection of citizens' rights in smart cities is the fact that fundamental rights and proportionality- thinking only take place within the limits of each specific smart city project. The section aims to explore the challenge of mapping and assessing smart cities' aggregated or cumulative effects on fundamental rights arising from the slow accumulation of different projects. Section 3.2.1 introduces the proportionality principle and explains why such effects are relevant to consider in smart cities. Section 3.2.2 then queries whether fundamental rights law, and especially data protection law, require or support an assessment of cumulative effects.

3.2.1 Challenges in applying proportionality in the smart city environment

PROPORTIONALITY PRINCIPLE AND THE CFR. The conditions which may legitimise limitations on fundamental rights in the EU legal order are set out in Article 52(1) CFR and include respect of the proportionality principle. The European Data Protection Supervisor has noted that for proportionality to be ensured, "the advantages resulting from the measure should not be outweighed by the disadvantages the measure causes with respect to the exercise of fundamental right".[147] Even though this Deliverable does not aim to provide a detailed analysis of the principle, for the ensuing discussion on cumulative effects it is important to briefly sketch the key notions underlying the principle. Firstly, proportionality entails a balancing exercise. To conduct this exercise one needs to establish the "degree of compression" or "intensity" of the interference with the right by the opposing interest, one the one hand, and the importance or legitimacy attached to the satisfaction of the opposing interest on the other hand.[148] Secondly, the

[147] EDPS, 'EDPS Guidelines on Assessing the Proportionality of Measures That Limit the Fundamental Rights to Privacy and to the Protection of Personal Data' (2019) 9.

[148] ibid 11; Lorenzo Dalla Corte, 'Safeguarding Data Protection in an Open Data World: On the Idea of Balancing Open Data and Data Protection in the Development of the Smart City Environment' (PhD Thesis, University of Tilburg 2020) 174.

analysis is always to be undertaken based on the facts of the specific case. A well-performed application of proportionality requires clarity and precision over the two elements to be considered in the balancing exercise.[149] Thirdly, while the principle is generally perceived as a key instrument of judicial methodology, since the proportionality test has indeed been articulated through case law, it is nowadays relevant well beyond the courtroom. Proportionality must be considered by the legislator when it develops legislative proposals to ensure that the proposed measure respects fundamental rights. Accordingly, it has "developed into a law-making tool".[150]

PROPORTIONALITY AND DATA PROTECTION. EU data protection law illustrates how proportionality can indeed permeate legislation. Dalla Corte argues that proportionality is "data protection's leitmotiv", a general and overarching value reflected in the several legal provisions that "require specific aspects of the processing to be suitable, necessary, and proportionate in light of the purposes set".[151] Proportionality thinking thus becomes relevant not only for courts and legislators, but also for the countless public and private entities called to comply with data protection law.

PROPORTIONALITY, SMART CITIES AND CUMULATIVE EFFECTS. if proportionality requires case-by-case assessments and clarity about the extent to which rights are compressed, on the one hand, and the importance of the sought objectives, on the other hand, it is only natural that assessments are confined within each specific project. Each project owner has knowledge about the impacts and importance of its own project, and can perform an assessment in consideration of these own factors. After all, there is no smart city as a legal entity[152] to which responsibility for balancing can be attributed.

This fragmented approach, while understandable from the perspective of placing legal responsibilities, leaves the question of the proportionality of the continuous interventions in the public space and governance unaccounted for. Smart city development may be fragmented, but experiences of living in the city are not. For the individual the city is an entity, a place for important social, economic and political activity. From the perspective of the individual and his or her rights, accumulation and the resulting "scaling" of smart city interventions may matter. The intensity of fundamental rights' interferences may change as a result of the accumulation of smart city projects.

[149] EDPS (n 147) 11.

[150] Dalla Corte (n 148) 170.

[151] ibid., 171.

[152] Sofia Ranchordás, 'Citizens as Consumers in the Data Economy: The Case of Smart Cities' [2018] EuCML 154, 157.

SCALE MAY IMPACT INTENSITY OF INTERFERENCES. If we take affronts to privacy as an example, previous sections argued that privacy is understood broadly as offering seclusion, but also, the freedom to self-develop, which especially in the smart city context translates to a freedom to act autonomously in the public space.[153] Interferences with privacy aggravate as projects accumulate. The more data processing technologies are embedded in public spaces, the less the possibility for seclusion. The less seclusion, the more the potential for chilling effects and for people to change their behaviour in public spaces. Equality rights are also a useful example. As more and more public services become digitalized, the issue of exclusion of certain citizens from city services becomes more severe.

SCALE MAY IMPACT CITIES POTENTIAL TO DELIVER THEIR PUBLIC INTEREST OBJECTIVES. On the other side of the balancing scale, where one needs to weigh in the importance of the pursued general interest objectives, and whether these can be effectively and efficiently fulfilled by the technology, accumulation also matters. Strands of smart city literature seem to insist that it is pervasive (rather than isolated) new technologies that can deliver smartness, and that cities should realise that "solving one [system] is not a viable long-term option" - a "holistic strategy" is required.[154]

As both the potential negative impacts, and the promised benefits, are affected by the slow accumulation of smart city projects, one may wonder whether proportionality analyses focused only on specific projects are adequate to address balancing challenges in the development of smart cities.

3.2.2 Lack of legal requirement(s) to assess possible cumulative effects

3.2.2.1 Fundamental rights law and pleas for holistic assessments of impacts of legislation

ACCUMULATION AND THE PRIVACY VS. SECURITY DEBATE. Taking a step back from the smart city context, it should be noted that the challenge of accumulation has already been raised in the context of the "privacy vs. security" debate that gained prominence after 9/11. The 9/11 attacks saw an increasing number of mass surveillance measures being adopted by the European and Member States legislators.[155] Authors have raised concerns over how, under the current understanding of the proportionality test, legislators and courts examine one law at a time. They argued that if each law is isolated from its surrounding legal and

[153] Galič (n 127) Chapter 7.

[154] Susanne Dirks and Mary Keeling, 'A Vision of Smarter Cities: How Cities Can Lead the Way into a Prosperous and Sustainable Future' (2009) Executive Report IBM Institute for Business Value.

[155] Article 29 Data Protection Working Party, 'Opinion 01/2014 on the Application of Necessity and Proportionality Concepts and Data Protection within the Law Enforcement Sector' (2014) WP 211 21.

factual situation, "the intrusion into the right to privacy caused by each individual law may well be found to be proportionate, although [laws] would be deemed disproportionate if viewed in combination".[156] This brings the risk that surveillance measures can grow continuously and practically unrestrictedly.[157] Provided that no single sweeping law disproportionately limits the right to privacy, several different laws could constitute legitimate and proportionate interferences with the right.

PLEAS FOR HOLISTIC ASSESSMENTS OF IMPACTS OF LEGISLATION. The challenge of accumulation and the need for a different approach when assessing interferences with rights have also been acknowledged beyond academia. The judgment of the German Constitutional Court, annulling provisions of the German act transposing the EU Data Retention Directive, is a striking example.[158] The Directive –and the ensuing national legislation- required the retention of telecommunications data for a period of six months to two years to enable their availability for law enforcement purposes. The Court held, among other things, that the German legislator "is obliged to exercise a greater restraint in considering new duties or authorities to store personal data with regard to the totality of the various existing data pools".[159] It has been argued that this statement amounts to the Court favoring a holistic approach, by which it considers that the entirety of existing surveillance measures and databases must be considered when the legislator plans to enact new data retention measures.[160] Discussing proportionality in the context of law enforcement-related personal data processing, Article 29 Working Party (WP29) has also affirmed that "it is necessary to assess how [a] new measure would add to the existing ones and whether all of them taken together would still proportionately limit the fundamental rights of data protection and privacy".[161]

A CHALLENGING TASK. However, neither the German Court nor WP29 explain how to proceed with such a holistic assessment. As for the literature, even though it stresses the need to move beyond the fragmented "one law at a time" approach, it accepts that evaluating surveillance holistically is a difficult task. There are nowadays so many laws introducing some form of surveillance for different parts

[156] Carolin Kaiser, 'Privacy and Identity Issues in Financial Transactions: The Proportionality of the European Anti-Money Laundering Legislation' (University of Groningen 2018) 549 <https://research.rug.nl/en/publications/privacy-and-identity-issues-in-financial-transactions-the-proport> accessed 9 April 2021.

[157] ibid., 553.

[158] BVerfG, 1 BvR 256/08 [2010].

[159] ibid., para. 218. The English translation of the excerpt is taken from Kaiser (n 148) 552.

[160] Franziska Boehm and Mark Cole, 'Data Retention after the Judgement of the Court of Justice of the European Union' (2014) Study funded by the Greens/EFA Group in the European Parliament 88.

[161] Article 29 Data Protection Working Party, 'Opinion 01/2014 on the Application of Necessity and Proportionality Concepts and Data Protection within the Law Enforcement Sector' (n 155) 22.

of the population (e.g. immigrants, passengers, tax-payers) that the full extent of measures and their impact is challenging to map.[162] To solve the conundrum, it has been proposed that "a trusted entity", such as the national data protection authority, could be tasked to undertake the mapping of the landscape of surveillance and make preliminary assessments about the seriousness of new interferences. Others have suggested to identify, for each piece of surveillance legislation, all actors who affect or are affected by it in order to come up with an "ecosystem" surrounding each law.[163] The same ecosystem exercise should be undertaken when new legislation is proposed. Looking at interconnections between the different ecosystems, and comparing existing ones with new ones, would make it possible to identify areas of overlap. Overlaps could hint to the existence of disproportionate effects, if for example it is revealed that some actors are repeatedly subjected to interferences with their right to privacy.[164]

A HERCULIAN TASK IN THE SMART CITY CONTEXT. The analysis above concerned cumulative effects of privacy-intrusive legislation. Any assessment of cumulative effects in smart cities is significantly more complex. In the case of smart city projects that entail the processing of personal data, a single piece of legislation (e.g. the GDPR, the Data Protection Law Enforcement Directive, national data protection acts) authorizes the emergence of multiple projects, and entrusts the assessment of possible impacts on rights to each data controller. For projects not processing personal data, as there is no dedicated legislation on matters such as algorithmic transparency and discrimination, nudging, and digital exclusion, any consideration of impacts again falls on the shoulders of project owners. In the smart city paradigm, there is no single legislator with knowledge of other existing laws and access to expert advice from data protection authorities, but numerous project owners implementing smart technologies often in an uncoordinated fashion. In such a multi-actor environment, mapping and assessing cumulative effects can be a herculean task.

3.2.2.2 The (missed) opportunity of data protection law

Conceptually, for reasons this section explains, compared to classic fundamental rights such as privacy or non-discrimination, the "modern" right to data protection found in Article 8 CFR offers more grounding for possible assessments of cumulative impacts in smart cities. The role of the right to data protection and its relationship with other rights have not yet been clearly addressed by courts, and still spark stimulating academic debates. However, a very interesting proposition

[162] Kaiser (n 156) 553.

[163] Lauren E Elrick, 'The Ecosystem Concept: A Holistic Approach to Privacy Protection' (2021) 35 International Review of Law, Computers & Technology 24, 37.

[164] ibid., 37-38.

has been recently made by Max von Grafenstein to conceptualise the right to data protection as a right meant to regulate (and protect against) risks of personal data processing against other fundamental rights.[165] The author argues that the right in Article 8 and secondary data protection law may embody certain concepts of the "precautionary principle" and the "risk-based approach".[166] A similar argument was made when the GDPR was adopted in 2016, when van Dijk et al. explained how the obligation to conduct a DPIA to assess "risks to the rights and freedoms of data subjects" essentially "epitomises the shift from classical legal practice to more risk-based approaches".[167]

Such risk-based approaches normally come to play as regulatory strategies when there are knowledge uncertainties.[168] There may not be enough knowledge to determine how likely it is that an event causes harm to a specific object of protection, and should harm occur, how severe that is. Or, there may be insufficient knowledge to prove who is responsible for a harm since the causality chain is unclear, because several actors and/or (their) actions may have contributed to a harm.[169] The precautionary principle and the risk-based approach denote that even in situations of uncertainty, protective measures ought to be taken before risks become fully apparent or turn into actual harm.[170] In other words, despite uncertainty, one can –and in fact should- act to prevent harm.

In data protection law this approach is mainly reflected in the DPIA. The DPIA requires controllers to assess the necessity and proportionality of their processing operations, identify risks to the fundamental rights and freedoms of data subjects, and propose measures to address such risks.[171] This is a departure from classical legal practice. Classic rights and the protection they afford are typically shaped through jurisprudence, after an alleged breach has taken place. Protection is mainly reactive. With data protection and the DPIA, the determination of the normative content of rights and the preoccupation to protect them become anticipatory, and no longer the sole task of courts. Data controllers also have to interpret and apply (risks to) rights. Moreover, the means to ensure protection also change. Protection is not to be achieved only by legislators or courts applying strict legal tools like the proportionality test. Impact Assessments, -the DPIA is indeed a form of Impact Assessment-, become an important protection strategy,

[165] von Grafenstein (n 123).

[166] ibid., 517-521.

[167] van Dijk, Gellert and Rommetveit (n 28) 286.

[168] von Grafenstein (n 123) 519–520.

[169] ibid., 521.

[170] Luiz Costa, 'Privacy and the Precautionary Principle' (2012) 28 Computer Law & Security Review 14, 16.

[171] Article 35(7) GDPR.

offering a more flexible tool. Their aim is not to sanction or vindicate, but to contribute to informed decision-making and the protection of societal concerns. As such, they: i) are a "best efforts obligation"; ii) are meant to be inclusive and allow various stakeholders to express what they see as "risks" of an envisaged initiative; iii) span across an initiative's full development-lifecycle and are even revisited where necessary because, for instance, "society changes, dangers evolve and knowledge grows".[172]

The above discussion is relevant because in smart cities, there are important knowledge uncertainties when it comes to the possible impacts of projects' gradual accumulation on fundamental rights. More knowledge is needed to understand how individuals view smart cities as a whole. But by focusing on "risks" and favouring stakeholder involvement, it can be argued that Impact Assessments may indeed offer an appropriate tool to map, explore and assess cumulative impacts.

Thus, at least at a conceptual level, data protection law seems to support possible cumulative effects assessments in smart cities. It embodies elements of precaution, which call for regulatory action even in the existence of uncertainties. It has created tools, such as the DPIA, which seem better suited to address the challenge of cumulative effects. However, data protection law does not go as far as to require more holistic or cumulative assessments of possible impacts. A DPIA is meant to assess the necessity, proportionality and risks created by an envisaged processing operation. Neither the GDPR or guidelines of data protection authorities mention a duty to consider its inter-relationship with other –existing and future- processing operations.

3.3 The involvement of the private sector and accountability deficits

PRIVATISATION. Smart cities are characterized by privatization [173]or externalisation.[174] Private entities are closely involved in the design and deployment of smart urbanism, because of constraints in funding and technological expertise in the public sector. While partnerships between public authorities and private entities are prevalent in the smart cities context, the involvement and extent of control granted to private entities, and associated

[172] Kloza and others (n 110) 2.

[173] Sofia Ranchordás (n 140); Esther Keymolen and Astrid Voorwindenb, 'Can We Negotiate? Trust and the Rule of Law in the Smart City Paradigm' (2020) 34 International Review of Law, Computers & Technology 233.

[174] Jean-Bernard Auby, *Droit de La Ville - Du Fonctionnement Juridique Des Villes Au Droit à La Ville* (2nd edn, LexisNexis 2016). The term "externalisation" may be more suitable to use given that, as Auby explains, in the majority of cases public services haven't privatised in the strict sense. Rather, what have taken place are schemes of externalization or partnership.

challenges, can vary considerably. Smart city projects can be driven by big tech companies, who are also data owners. Such big "strategic" partners could also influence future procurement by being in a position to create technology procurement needs for which only specific companies could be sole source providers.[175] Data power and the ability to influence procurement create difficulties for (smaller) service providers that may be driven out of the market.[176] Besides questions of size and data and/or market power, companies of all sizes can design and sell, via a procurement process, technologies which as explained above carry risks to the enjoyment of a series of fundamental rights in cities. It then follows the risk that companies, and not local public authorities, become the decision-makers and "problem-solvers" in the smart city environment.[177]

The externalization encountered in smart cities poses two main sets of challenges on accountability. The first relates to the accountability principle under the GDPR stricto sensu, which requires, as explained in Section 1, data controllers to be responsible for, and be able to demonstrate compliance with data protection law –including its risk-based and balancing mechanisms (Sect. 3.3.1). The second relates to public accountability more broadly, and its links with legality, legitimacy and participation, understood for the purposes of this Deliverable as public authorities' obligation to protect the public interest and citizens' rights and be held accountable for their decisions to citizens (Sect. 3.3.2).

3.3.1 Accountability under the GDPR: private sector involvement and the challenge of enforcing data protection

DATA PROTECTION ROLES AND RESPONSIBILITIES. The GDPR places responsibilities on controllers and processors. Actors who do not fall under the controller or processor category but may nevertheless still influence data processing, such as software developers, developers of sensors, are not directly bound by data protection law.[178] As the accountability principle binds controllers, controllers have significantly more responsibilities for data protection than processors and other third parties, for they are the ones deciding on the purposes and means of the processing.

---

[175] Ellen Goodman and Julia Powles, 'Urbanism Under Google: Lessons from Sidewalk Toronto' (2019) 88 Fordham Law Review 457, 470–471.

[176] Laurens Vandercruysse and others, 'Public Procurement of Smart City Services: Matching Competition and Data Protection' (2020) Spectre Project Deliverable 41.

[177] Vasilis Niaros, 'Introducing a Taxonomy of the "Smart City": Towards a Commons-Oriented Approach?' (2016) 14 tripleC: Communication, Capitalism & Critique. Open Access Journal for a Global Sustainable Information Society 51.

[178] Rob Heyman, Jonas Breuer and Athena Christofi, 'Mapping and Modelling of the Smart Cities Ecosystem and Defining Responsibilities for Smart Cities' (2020) Spectre Project Deliverable 13.

WHO IS THE REAL CONTROLLER? While cities often remain controllers, or join-controllers, of the data collected for smart city purposes, the data is collected and processed by private parties - typically app developers, or service providers.[179] The risk of such processing activities should be determined prior to processing, and before the smart city project has started:[180] but smart cities projects are constantly evolving, and new risks arise that required new assessment and mitigation strategies. It is thus the city as a controller that decides whether the measures should be updated, but implementing these measures in an effective and feasible manner is the task of the processor. Furthermore, following Article 26(3) GDPR, data subjects should be able to claim their rights by *controller,* which is not effective if the controller, in this case mostly the city, is unaware of how processing takes place: from this practical perspective, it may be beneficial to have joint controllership between the city and private companies, yet this again raises the question in whose interests will such a joint controllership-arrangement act. From the perspective accountability, risk assessment and risk management should be a multi-actors exercise: [181] hence, if the city is a controller, service providers who are processors should be sufficiently involved, and vice-versa. The problem is that accountability is connected to decision-making power, while cities may lack technical capacity to actually make these decisions meaningful. In practice it can be particularly challenging for controllers to exert control vis-à-vis developers and processors and to monitor compliance. Doing so requires high levels of data literacy, as well as transparency and openness about the different technologies and processing operations at stake. The latter could nevertheless create tensions with confidentiality and intellectual property rights.

ACCOUNTABILITY AND COMPLEX, CHANGING TECHNOLOGIES. Smart cities also heavily rely on emerging technologies, especially when it comes to facilitating the speed of data collection.[182] The use of these technologies can transform our understand of data protection. These technologies are largely based on machine learning and algorithmic decision-making and are likely to introduce new actors in smart city ecosystem, fragmenting their responsibilities across different segments of technologies and rendering accountability even more challenging.

---

[179] Vandercruysse and others (n 176).

[180] Shakila Bu-Pasha, 'The Controller's Role in Determining "High Risk" and Data Protection Impact Assessment (DPIA) in Developing Digital Smart City' 29 Information & Communications Technology Law 391.

[181] Katerina Demetzou (2019) GDPR and the Concept of Risk: The Role of Risk, the Scope of Risk and the Technology Involved, in: Kosta E., Pierson J., Slamanig D., Fischer-Hübner S., Krenn S. (eds) Privacy and Identity Management. Fairness, Accountability, and Transparency in the Age of Big Data. Privacy and Identity 2018. IFIP Advances in Information and Communication Technology, vol 547. Springer, Cham, 149.

[182] Esther Keymolen and Astrid Voorwindenb, 'Can We Negotiate? Trust and the Rule of Law in the Smart City Paradigm' (2020) 34 International Review of Law, Computers & Technology 233, 238.

In this regard, Bu-Pasha examined whether there is a high risk to the rights and freedoms in the context of 5G and IoT used in smart cities. These technologies enable connections of sensors, exchange of information and reactions based on them, transfer data and communicate with other systems on an automatic level and without human interference,[183] which will form essential infrastructural components in smart cities. While yet to be introduced on the global scale, these technologies may change later on, and the risks they entail may become increasingly far-reaching. In practice, it means that DPIAs will have to be renewed each time there is a significant update to technology, and especially when the processing activities used in these technologies result in high risk.

The changes in the use of smart technologies may also change our understanding of the concepts of controller. Urquhart and Chen highlight that due to the emergence of smart homes, household occupants may be jointly responsible for GDPR compliance since they determine the means and purposes of data collection with IoT device vendors:[184] the emergence of these "domestic data controllers," division of responsibility and accountability in smart homes more challenging. Naturally, smart homes are different than smart cities, but the questions of the dynamics between controllers and the changing roles due to the IoT technologies are likewise present in the smart cities ecosystem; in Urquhart and Chen language, " the law is moving to the city,"[185] where responsibilities and dynamics between city actors become important. "(...) if a contract substantially gives one an entity material powers to decide how data is processed, but formally only assigns a different entity with less influence as a sole controller, such an assignment would be invalid and the former entity would remain liable as a joint controller."[186]

3.3.2 Accountability beyond the GDPR: trust and democratic oversight of smart city technologies

PRIVATE VENDORS AND PUBLIC ACCOUNTABILITY. Beyond issues of accountability under data protection law, the involvement of private companies in the design and deployment of smart city solution raises questions on public accountability more broadly. Several scholars have explored the tension between public and private values and interests in smart cities. Ranchordas and Klop have argued that privately-designed black box technologies used to automate urban law and

[183] Bu-Pasha (n 180).

[184] Urquhart and Chen (n 38).

[185] ibid., 4.

[186] ibid., 13.

policies can impede public authorities from exercising their duties to transparency and reason-giving, making accountability difficult. Researching on procurement practices in the United States about the acquisition of machine learning systems in the public sector, Mulligan and Bamberger have noted that public authorities have no knowledge or influence on the design of such systems and whether they align with public values. Brauneis and Goodman' s research has shown that aggressive trade secrets and confidentiality claims are invoked by private companies to limit the provision of information that is particularly meaningful for public authorities to have to understand the workings of these systems. Private companies thus have significant powers in shaping cities' transition into smart. Yet, decision-making in companies is driven by commercial considerations rather than by the interests of citizens, despite the fact that many companies have been recently making efforts to gain citizens' trust.[187]

ACCOUNTABILITY AND CITIZENS' PARTICIPATION. Another important challenge in the smart city environment is ensuring accountability through citizens' involvement. Keymolen and Voorwinden suggest that current participation mechanisms for citizens in smart cities are insufficient to contribute to political community and ensure political participation and allowing a say in city's affairs and when essential decision should be made that affect divergent interests (they refer to this puzzle as a "conflict"). Participation in smart cities revolves around data and data-driven applications citizens can use, or their data being shared through mobile applications, which, again, are mostly supplied by private actors.[188] Citizens contribute to smart cities by providing data (either through consent, or through providing data themselves) e.g. through security apps[189] rather than through participation in the decision-making processes. Such a "participation" does not provide room for citizen empowerment. To illustrate, critique on lack of citizens involvement and lack of transparency was voices with regard to the Ontario Sidewalk Lab, where the lobby efforts of private companies created accountability and transparency gaps and raised democratic control issues of misbalance between private and citizens interests.[190] In this regard, transparency may also be difficult to achieve in smart cities because contracts between cities and service

[187] See e.g. the creation of programmes such as Microsoft's AI for Good.

[188] Esther Keymolen and Astrid Voorwindenb, 'Can We Negotiate? Trust and the Rule of Law in the Smart City Paradigm' (2020) 34 International Review of Law, Computers & Technology 233, 238. Julsrud and Krogstad offer analysis of use of mobile phone data in Oslo and Estonia and in the context of citizen's trust, Tom Erik Julsrud and Julie Runde Krogstad (2020) Is there enough trust for the smart city? exploring acceptance for use of mobile phone data in oslo and Tallinn, Technological Forecasting and Social Change 161.

[189] E.g. The London Eye Security app

[190] Esther Keymolen and Astrid Voorwindenb, 'Can We Negotiate? Trust and the Rule of Law in the Smart City Paradigm' (2020) 34 International Review of Law, Computers & Technology 233, 248.

providers are usually not placed in public domain, which makes it challenging for citizens to learn which data is collected, how it is processed and where it is stored (since these issues are usually tackled in the contracts).

CONCLUSION: ENHANCING AND LEGITIMISING DATA PROTECTION IN SMART CITIES

This report explored the regulatory nature of the GDPR, in particular its emphasis on risks and on the accountability of controllers. This was done with a view to examine potential weaknesses of this approach in achieving –through the effective application and monitoring of data protection law- the protection of citizens' fundamental rights.

General challenges applicable to most data processing contexts include the limited resources for supervision and enforcement granted to DPAs, and the limited role data subjects and their representatives can play when it comes to the identification, assessment and monitoring of the risks a data processing operation could entail on fundamental rights. Currently, effective protection relies heavily on the good will of controllers. In the absence of strong scrutiny by DPAs, individuals and civil society, it is perhaps utopian to assume that controllers will leave up to the high GDPR standards.

When it comes to the effective protection of citizens' rights in smart cities, three additional challenges have been discussed in this report. The first relates to the complex nature of the rights that may be engaged in smart city initiatives, and the difficulty of identifying risks to rights without resorting to interdisciplinary and participatory exercises meant to gather and understand citizens' perceptions of smart technologies in the city. The second concerns the issue of assessing possible cumulative effects on rights, arising from the slow accumulation of smart city initiatives within a city. Finally, the close involvement of private companies in the design and development of smart city initiatives challenges the GDPR's accountability principle, but also the public accountability of public authorities to pursue the public interest and protect citizens' rights more broadly.

The analysis sets the ground to examine, in future reports (Deliverables 1.6 and 4.7) theoretical frameworks and on-the-ground measures to increase citizens' protection in smart cities, starting from but also going beyond the GDPR.

Firstly, we will examine how Article 35(9) GDPR can be used in smart cities to enable participation of citizens and/or their representatives in the identification and assessment of the risks of smart city technologies. Lessons from other types of Impact Assessments, in particular Environmental Impact Assessments and Constructive Technology Assessments will be used to discuss the benefits and modalities of participation and whether DPIAs should also embrace public participation, in particularly in the smart city context.

Secondly, we will explore solutions to the challenge of mapping and understanding cumulative effects in smart cities. Here too, inspiration can be found in the environmental law area given that the problem of accumulation is particularly acute there: environmental degradation is often the result of multiple actions, rather than a singular one. Therefore, it is important to reflect on whether similar processes to those used to understand and mitigate cumulative effects on the environment could be useful to provide an understanding of the cumulative effects on fundamental rights which slowly emerge as our cities become smart.

Thirdly, we will discuss the extent to which (and how) public contracts can be leveraged to increase data protection in smart cities and provide more democratic oversight over private vendors designing and deployment smart city technologies.

BIBLIOGRAPHY

Alvarez Rigaudias C and Spina A, 'Article 36. Prior Consultation' in Christopher Kuner, Lee A Bygrave and Christopher Docksey (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (2020)

Article 29 Data Protection Working Party, 'Opinion 01/2014 on the Application of Necessity and Proportionality Concepts and Data Protection within the Law Enforcement Sector' (2014) WP 211

——, 'Statement on the Role of a Risk-Based Approach in Data Protection Legal Frameworks' (2014) WP 218

——, 'Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing Is "Likely to Result in a High Risk" for the Purposes of Regulation 2016/679' (2017) WP 248 rev.01

Auby J-B, *Droit de La Ville - Du Fonctionnement Juridique Des Villes Au Droit à La Ville* (2nd edn, LexisNexis 2016)

Baldwin R, Cave M and Lodge M, *Understanding Regulation: Theory, Strategy, and Practice* (2nd Edition, Oxford University Press 2012)

Barocas S and Selbst AD, 'Big Data's Disparate Impact' (2016) 104 California Law Review 671

Beck U, 'Risk Society Revisited: Theory, Politiques, Critiques and Research Programmes' in Barbara Adam, Ulrich Beck and Joost van Loon (eds), *The Risk Society and Beyond: Critical Issues for Social Theory* (SAGE 2012)

Bennett C and Raab C, *The Governance of Privacy* (Ashgate Publishing)

Binns R, 'Data Protection Impact Assessments: A Meta-Regulatory Approach' (2017) 7 International Data Privacy Law 22

Boehm F and Cole M, 'Data Retention after the Judgement of the Court of Justice of the European Union' (2014) Study funded by the Greens/EFA Group in the European Parliament

Bu-Pasha S, 'The Controller's Role in Determining "High Risk" and Data Protection Impact Assessment (DPIA) in Developing Digital Smart City' 29 Information & Communications Technology Law 391

Christofi A and others, 'Erosion by Standardisation: Is ISO/IEC 29134:2017 on Privacy Impact Assessment Up to (GDPR) Standard?' in Maria Tzanou (ed), *Personal Data Protection and Legal Developments in the European Union* (IGI Global 2020)

Clifford D, 'The Legal Limits to the Monetisation of Online Emotions' (PhD Thesis, KU Leuven 2019)

Clifford D and Ausloos J, 'Data Protection and the Role of Fairness' (2018) 37 Yearbook of European Law 130

Cohen JE, 'Turning Privacy Inside Out' (2019) 20 Theoretical Inquiries in Law <https://www7.tau.ac.il/ojs/index.php/til/article/view/1607> accessed 7 June 2021

Costa L, 'Privacy and the Precautionary Principle' (2012) 28 Computer Law & Security Review 14

Craig P, 'Right to Good Administration' in Steve Peers and others (eds), *The EU Charter of Fundamental Rights: A Commentary* (Hart Publishing 2014)

Dalla Corte L, 'Safeguarding Data Protection in an Open Data World: On the Idea of Balancing Open Data and Data Protection in the Development of the Smart City Environment' (PhD Thesis, University of Tilburg 2020)

Demetzou K, 'Data Protection Impact Assessment: A Tool for Accountability and the Unclarified Concept of "High Risk" in the General Data Protection Regulation' (2019) 35 Computer Law & Security Review 105342

DIGITALEUROPE, 'Response to Public Consultation on Draft EDPB Guidelines on Codes of Conduct and Monitoring Bodies' (4 May 2019) <https://www.digitaleurope.org/resources/response-to-public-consultation-on-draft-edpb-guidelines-on-codes-of-conduct-and-monitoring-bodies/>

Dirks S and Keeling M, 'A Vision of Smarter Cities: How Cities Can Lead the Way into a Prosperous and Sustainable Future' (2009) Executive Report IBM Institute for Business Value

Downes L, *The Laws of Disruption: Harnessing the New Forces That Govern Life and Business in the Digital Age* (Basic Books 2009)

EDPS, 'EDPS Guidelines on Assessing the Proportionality of Measures That Limit the Fundamental Rights to Privacy and to the Protection of Personal Data' (2019)

Elrick LE, 'The Ecosystem Concept: A Holistic Approach to Privacy Protection' (2021) 35 International Review of Law, Computers & Technology 24

European Union Agency for Fundamental Rights, 'Access to Data Protection Remedies in EU Member States' (2013)

Finch K and Tene O, 'Welcome to the Metropticon: Protecting Privacy in a Hyperconnected Town Symposium: Smart Law for Smart Cities: Regulation, Technology, and the Future of Cities' (2013) 41 Fordham Urban Law Journal 1581

Galič M, 'Surveillance and Privacy in Smart Cities and Living Labls: Conceptualising Privacy for Public Space' (University of Tilburg 2019) <https://research.tilburguniversity.edu/en/publications/surveillance-and-privacy-in-smart-cities-and-living-labs-conceptu>

Gellert R, 'Understanding the Notion of Risk in the General Data Protection Regulation' (2018) 34 Computer Law & Security Review 279

——, *The Risk-Based Approach to Data Protection* (Oxford University Press 2020)

González Fuster G, 'Article 80. Representation of Data Subjects' in Christopher Kuner, Lee A Bygrave and Christopher Docksey (eds), *The General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020)

Goodman E and Powles J, 'Urbanism Under Google: Lessons from Sidewalk Toronto' (2019) 88 Fordham Law Review 457

Heyman R, Breuer J and Christofi A, 'Mapping and Modelling of the Smart Cities Ecosystem and Defining Responsibilities for Smart Cities' (2020) Spectre Project Deliverable 13

Hijmans H, 'Article 57. Tasks' in Christopher Kuner, Lee A Bygrave and Christopher Docksey (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020)

Insurance Europe, 'Response to the EDPB's Draft-Guidelines on Codes of Conduct & Monitoring Bodies, Position Paper Referring to Guidelines 1/2009 on Codes of Conduct & Monitoring Bodies under Regulation 20116/679' (4 October 2019) <https://www.insuranceeurope.eu/sites/default/files/attachments/Response%20to%20EDPB%20draft-guidelines%20on%20codes%20of%20conduct%20%26%20monitoring%20bodies.pdf>

Jameson S, Richter C and Taylor L, 'People's Strategies for Perceived Surveillance in Amsterdam Smart City' [2019] Urban Geography 1

Kaiser C, 'Privacy and Identity Issues in Financial Transactions: The Proportionality of the European Anti-Money Laundering Legislation' (University of Groningen 2018) <https://research.rug.nl/en/publications/privacy-and-identity-issues-in-financial-transactions-the-proport> accessed 9 April 2021

Kamara I, 'Co-Regulation in EU Personal Data Protection: The Case of Technical Standards and the Privacy by Design Standardisation "Mandate"' (2017) 8 European Journal of Law and Technology <https://ejlt.org/index.php/ejlt/article/view/545> accessed 4 June 2021

——, 'Article 40. Codes of Conduct' in Christopher Kuner, Lee A Bygrave and Christopher Docksey (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020)

Keymolen E and Voorwindenb A, 'Can We Negotiate? Trust and the Rule of Law in the Smart City Paradigm' (2020) 34 International Review of Law, Computers & Technology 233

Kitchin R, 'The Ethics of Smart Cities and Urban Science' (2016) 374 Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences 20160115

Kloza D and others, 'Data Protection Impact Assessments in the European Union: Complementing the New Legal Framework towards a More Robust Protection of Individuals' (d.pia.lab Policy Brief No 1 2017)

Koops B-J, 'The Trouble with European Data Protection Law' (2014) 4 International Data Privacy Law 250

——, 'A Typology of Privacy' (2017) 38 University of Pennsylvania Journal of International Law 483

Kotschy W, 'Article 78. Right to an Effective Judicial Remedy against a Supervisory Authority' in Christopher Kuner, Lee A Bygrave and Christopher Docksey (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020)

Lazaro C and Métayer DL, 'Control over Personal Data: True Remedy or Fairy Tale?' (2015) 12 SCRIPTed 3

Leenes R, 'Article 42. Certification' in Christopher Kuner, Lee A Bygrave and Christopher Docksey (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020)

Lodge M and Wegrich K, *Managing Regulation: Regulatory Analysis, Politics and Policy* (Palgrave Macmillan 2012)

Lynskey O, *The Foundations of EU Data Protection Law* (2015)

Macenaite M, 'The "Riskification" of European Data Protection Law through a Two-Fold Shift' (2017) 8 European Journal of Risk Regulation 506

Morton A and others, '"Tool Clinics" – Embracing Multiple Perspectives in Privacy Research and Privacy-Sensitive Design' in Alessandro Acquisti and others (eds), *My Life, Shared - Trust and Privacy in the Age of Ubiquitous Experience Sharing* (Dagstuhl Reports 2013)

Niaros V, 'Introducing a Taxonomy of the "Smart City": Towards a Commons-Oriented Approach?' (2016) 14 tripleC: Communication, Capitalism & Critique. Open Access Journal for a Global Sustainable Information Society 51

Parker C, *The Open Corporation: Effective Self-Regulation and Democracy* (Cambridge University Press 2002)

Pierson J, 'Online Privacy in Social Media: A Conceptual Exploration of Empowerment and Vulnerability.' [2012] Communications & Strategies 99

Ponce J, 'Good Administration and Administrative Procedures' (2005) 12 12 Indiana Journal of Global Legal Studies 551 (2005) <https://www.repository.law.indiana.edu/ijgls/vol12/iss2/10>

Quelle C, 'Enhancing Compliance under the General Data Protection Regulation: The Risky Upshot of the Accountability- and Risk-Based Approach' (2018) 9 European Journal of Risk Regulation 502

Ranchordás S, 'Citizens as Consumers in the Data Economy: The Case of Smart Cities' [2018] EuCML 154

——, 'Smart Mobility, Transport Poverty and the Legal Framework of Inclusive Mobility' in Michèle Finck and others (eds), *Smart Urban Mobility: Law, Regulation, and Policy* (Springer 2020) <https://doi.org/10.1007/978-3-662-61920-9_4> accessed 12 March 2021

——, 'The Digitalization of Government and Digital Exclusion: Setting the Scene' (University of Groningen Faculty of Law 2020) Research Paper Series No. 30/2020

Selznick P, 'Focusing Organizational Research on Regulation' in Roger Noll (ed), *Regulatory Policy and the Social Sciences* (University of California Press 1985)

Sofia Ranchordás, 'Law and Autonomous Systems Series: Cities as Corporations? The Privatization of Cities and the Automation of Local Law' (*Oxford Business Law Blog*, 18 April 2018) <https://www.law.ox.ac.uk/business-law-blog/blog/2018/04/law-and-autonomous-systems-series-cities-corporations-privatization> accessed 12 March 2021

Urquhart L and Chen J, 'On the Principle of Accountability: Challenges for Smart Homes & Cybersecurity' (2020) Paper available at SSRN

van Dijk N, Gellert R and Rommetveit K, 'A Risk to a Right? Beyond Data Protection Risk Assessments' (2016) 32 Computer Law & Security Review 286

Vandercruysse L and others, 'Public Procurement of Smart City Services: Matching Competition and Data Protection' (2020) Spectre Project Deliverable 41

von Grafenstein M, 'Refining the Concept of the Right to Data Protection in Article 8 ECFR – Part I' (2020) 6 European Data Protection Law Review 509

Yeung K and Bygrave LA, 'Demystifying the Modernized European Data Protection Regime: Cross-Disciplinary Insights from Legal and Regulatory Governance Scholarship' Regulation & Governance