Areas of Tension in the Application of AI and Data Protection Law

On the Lack of Substantive Balancing and Coordinated Legal Concretisation in the European Commission's Proposal for a Regulation on AI

*Mona Winau**

The contribution considers specific challenges that arise from a parallel applicability of AI and Data Protection Law regarding the European Commission's Proposal for a Regulation laying down harmonised rules on Artificial Intelligence (AI Act) and the EU General Data Protection Regulation (GDPR). The legal analysis is based on a consideration of overlapping regulatory objectives and subject matters, with at the same time fundamentally different regulatory concepts and conflicting regulatory goals in concrete terms. Taking an example of the providers' obligations to assure accuracy of the system and to make sure that training, validation and testing data sets are relevant, representative, free of errors and complete on the one hand and the limitations on processing personal data due to the data minimisation principle on the other, this article highlights that legal provisions from the AI Act and the GDPR must be interpreted and applied in accordance with their respective regulatory goals, but with consideration for each other. From that it is deduced that a coherent, and thus efficient, application of both legal acts depends on a substantive balance in areas of tension between AI regulation and data protection law. The author argues that the balancing is an essential matter and that the mere coexistence of AI and Data Protection Law as provided for in the Commission's proposal does not suffice.

Keywords: Product Safety Law | Data Minimisation | Accuracy | Data Governance | Harmonised Standards

I. Introduction

With its proposal for a Regulation laying down harmonised rules on Artificial Intelligence (AI Act), the EU Commission has presented a horizontal regulation that is intended to promote innovation in the AI sector, safeguard a free market for AI systems, and at the same time, ensure that AI systems are developed and used in accordance with Union Law, fundamental rights, freedoms, and values.[1] Comparable regulatory objectives are also pursued by the General Data Protection Regulation (GDPR) which has applied in the EU since 2018. The two regulations overlap in their scope of application due to the processing of personal data in AI systems. However, the AI Act does not explicitly deal with its relationship to the GDPR.[2] Only in the Explanatory Memorandum to the AI Act is it clarified that it is without prejudice and complements the GDPR.[3] However, in concrete

DOI: 10.21552/edpl/2023/2/7

* Karlsruhe Institute of Technology. For Correspondence: <mona.winau@kit.edu>. This research is supported by the topic Methods for Engineering Secure Systems of the Helmholtz Association (HSF) and by KASTEL Security Research Labs.

1 EU Commission Proposal for a Regulation laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts [2021] 0106(COD), Explanatory Memorandum [1.1].

2 Unlike the Regulation (EU) 2018/1724 of 2 October 2018 establishing a single digital gateway to provide access to information,

terms, areas of tension arise between objectives and obligations following from the AI Act on the one hand and the GDPR on the other hand. In the following it is argued that interpretation and application of such conflicting legal norms must be done in coordination with each other to enable effective application of both acts, but that the Commission's proposal does not address this. The legal analysis herein starts with a consideration of the overlapping regulatory objectives and scopes of application of the AI-Act and the GDPR (II). Subsequently the main differences of the chosen regulatory concepts of both legal acts are outlined (III). In section (IV) a model of conflicting obligations regarding a high-risk AI system, intended to be used for the selection of application for jobs, that is based on training with personal data is used to exemplify areas of tension. Finally, it is posited that there is a need for substantive provisions to balance colliding legal norms in AI regulation and data protection law or at least for procedural safeguards in the procedures of concretisation of the law to ensure a coherent interpretation and application (V).

II. Overlapping Areas of Application and Regulatory Objectives

Looking only at the subject matter of regulation, the GDPR covers regulation for the processing of personal data, regardless of the processing method and purpose (Art. 2 par. 1).[4] The AI Act addresses the placing on the market, the putting into service and the use of so called Artificial Intelligence (AI) systems (Art. 2 par. 1 AI Act), including the processing of personal and/or non-personal data by those systems. According to Art. 5 par. 1 lit. a AI-Act, this does not refer to a specific technical processing method. Rather it is a broad generic term for various automated (algorithm-based) processing methods the result of which is an output for a given set of human-defined objectives.[5] Compared to GDPR its reference point is broader regarding the reference to persons, but narrower in regard to the methods and purposes of processing. Consequently, the matters overlap when personal data are processed in an AI system. Considering this, it seems consistent that the regulatory purposes also show substantial parallels. As Art. 1 par 1 of GDPR shows, Data Protection law aims to guarantee a free movement of personal data as well as to protecting fundamental rights and freedoms of natural persons from risks resulting from the processing of personal data. The proposal for a European AI Act is intended to create a uniform legal framework for the development, marketing, and use of AI systems to ensure the free movement of AI based goods and services and to protect public interests, which explicitly include the protection of individual fundamental rights (Rec. 1). Therefore, both regulations intend to strike a proportional balance between, on the one hand, the guarantee of the free market and the protection of economic and public interests in the processing of personal data respectively in the use of so called Artificial Intelligence, and on the other hand, the protection of Union values, fundamental rights and principles jeopardised by the former.[6]

If a practical context in connection with an AI system is considered, the AI Act covers at least two levels from which a risk to the values and fundamental rights to be protected may result. An AI system is developed or produced in a first step and used in practice in a second step.[7] When an AI system that is con-

to procedures and to assistance and problem-solving services and amending Regulation (EU) No 1024/2012 (Data Governance Act) [2018] OJ L295/1 and the EU Commission Proposal for a Regulation of 23 February 2022 on harmonised rules on fair access to and use of data (Data Act) Data Act [2022] 0047(COD) recently submitted by the EU Commission the AI Act does not contain a conflict-of-law rule regarding data protection law. Due to Art. 1 (2) Data Governance Act the Regulation is without prejudice to Union legal acts related to the processing of personal data. According to Art. 1 (3) Data Act it does not affect the applicibilty of EU data protection law.

3 COM Proposal AI Act (n 2), Explanatory Memorandum [1.2].

4 Art. 2 par. 1 GDPR limits refers to the processing method insofar as it applies to the *processing of personal data wholly or partly by automated means* or by non-automated means of *personal data which form part of a filing system or intended to form part of a filing system*.

5 In more detail and critical regarding the definition in Art. 5 (1) lit. a of the Commission's proposal, Martin Ebers and others, 'The European Commission's Proposal for an Artificial Intelligence Act – A Critical Assessment by Members of the Robotics and Ai Law Society' [2021] Mutlidisciplinary Scientific Journal 589, 590. As the provisions of the regulation apply to specified types of AI systems, this is not particularly significant, cf. Michael Veale and Frederik Zuiderveen Borgesius, 'Demystifying the Draft EU Artificial Intelligence Act' [2021] CRi 97, 109; Natalie A. Smuha and others, 'How the EU Can Achieve Legally Trustworty AI: A Response to the European Commission's Proposal for an Artificial Intelligence Act [2021] 14 SSRN Journal <https://www.ssrn.com/abstract=3899991> accessed 15 June 2023.

6 Rec. 4 GDPR; COM Proposal AI Act (n 2) Expalantory Memorandum [1.1].

7 Even the development of an AI system often covers different steps and involves several actors, Mattis Jacobs and Judith Simon, 'Assigning Obligations in AI Regulation: A Discussion of Two Frameworks Proposed by the European Commission' [2022] DISO 6, 9pp.

sidered to be high-risk by Art. 6 AI Act is developed, the obligations from Title III Chapter 2, which mainly address the provider (Art. 16),[8] apply.[9] If personal data are processed as the system is developed, GDPR will also apply towards the provider as a controller (Art. 4 No. 7 GDPR). Due to Art. 4 No. 1 GDPR data is personal if a person can be identified by it. Identifiability is a broad and dynamic term.[10] Data that has not been personal when it has been collected can turn into personal data during its lifetime if additional information that is likely to be used to identify a person becomes available.[11] Additionally it should be considered that, at least for learning AI systems, data is usually processed in two steps, for training and validation purposes, and only a small amount of personal data in one of the data sets that is not separated from other anonymous data processed is enough to trigger the application of GDPR.[12] Thus it seems to be the standard case that personal data is processed.[13]

An AI system that has been placed on the market or put into service can in a next step be purchased and used. Towards the user there are only a view obligations from Art. 29 such as using the AI system in accordance with the instruction of use (par. 1) and ensuring that input data is relevant in view of the intended purpose to the extent he exercises control (par. 3).[14]

If the system interacts with its environment more personal data will be processed while using it. One thinks of intelligent video surveillance systems processing biometric data (Annex III No. 1) or systems used for recruitment or selection in an employment context (Annex III No. 4a). In such cases GDPR also applies.

Depending on who determines purposes and means of a concrecte processing operation, the provider and the user could be the controller in terms of Art. 4 No. 7 GDPR alone or in joint controllerschip. If the user is the single controller, the provider could also be a processor according to Art. 4 No. 8 GDPR.

In conclusion, it is most likely that obligations from the AI Act and GDPR will apply parallel to the same actor (provider and/or user) when an AI system is developed and used in practice.[15] In any case, in practice connected circumstances, will regularly be covered by both laws, namely the design, development and use of a high-risk AI system.

III. Differences in Regulatory Approaches

Unlike the fairly similiar regulatory objectives and subjects, there are some key differences in the regulatory concepts in the GDPR and the AI Act. In the following section, the main differences in the chosen approaches and in the procedures of concretising the law to ensure an effective application, not including complementary member state legislation, jurisprudence, and academia, are pointed out.

8 See also in regard to the main responsibility of the provider, *Veale and Borgesius Zuiderveen* (n 6) 102p; Gabriele Mazzini and Salvatore Scalzo, 'The Proposal for the Artificial Intelligence Act: Considerations around Some Key Concepts' [2022] 4 SSRN Journal <https://www.ssrn.com/abstract=4098809> accessed 15 June 2023. The focus of the provider as the regulatory addressee differs from the Commission's intention to address the actor who is best placed to be, *Jacobs and Simon* (n 8) 7.

9 Furthermore, special obligations arise towards product manufacturers (Art. 24), authorised representatives (Art. 25), importers (Art. 26), distributors (Art. 27) and users (Art. 29).

10 Rec. 26 S. 3 states: 'To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly.' This refers to the ECJ jurisprudence in the Case C-582/14 *Breyer* [2016] 62014CJ0582, par.42pp. See also in regard to identifiability, Lilian Mitrou, 'Data Protection, Artificial Intelligence and Cognitive Services: Is the General Data Protection Regulation (GDPR) 'Artificial Intelligence-Proof'?' [2018] 28 SSRN Journal 28 <https://www.ssrn.com/abstract=3386914> accessed 15 June 2023.

11 *Mitrou* (n 11) 28 p; cf. regarding the development of data to personal data, Nadezhda Purtova, 'The Law of Everything' Law, Innovation and Technology [2018] 40; regarding the prossibility of re-identification of anonymised training data, Philipp Hacker, 'A Legal Framework for AI Training Data – From First Principles to the Artificial Intelligence Act' Law, Innovation and Technology [2021], 257, 265ff.

12 Indra Spiecker gen. Döhmann, 'AI and Data Protection' in Larry A. Di Matteo, Cristina Poncibò and Michel Cannarsa (eds), *The Cambridge Handbook of Artificial Intelligence: Global Perspectives on Law and Ethics* (Cambridge University Press 2022) 132, 133p.

13 In regard to the double-sided relationship of AI systems and the processing of personal data also *Mitrou* (n 11) 19; Jozef Andrasko, Matus Mesarcik and Ondrej Hamulak, 'The Regulatory Intersection Between Artificial Intelligence, Data Protection and Cyber Security: Challenges and Opportunities for the EU Legal Framework' [2021] AI & Society 623, 628. Dissenting with regard to training data more generally, *Hacker* (n 12) 268.

14 The harmonised regulation of the product use is a speciality of the AI Act that was considered to be necessary for AI systems. Usually, product safety law based on the NLF does not cover obligations for users, *Mazzini and Scalzo* (n 9) 9.

15 See also *Mazzini and Scalzo* (n 9) 14p; Ferhana Ferdousi Liza, 'Challenges of Enforcing Regulation in Artificial Intelligence Act' (Proceedings of the 2022 1st International Workshop on Imaging the AI Landscape After the AI Act 3) <https://ueaeprints.uea.ac.uk/id/eprint/85717/> accessed 15 June 2023. Regarding the scope of application of GDPR, *Mitrou* (n 11) 27p; *Andrasko, Mesarcik and Hamulak* (n 14) 628.

1. Key Differences in Regulatory Concepts

While the EU Commission's proposal for an AI-Act is a classic product safety law based on the European New Legislative Framework (NLF); the GDPR sets out a framework on whether and how personal data are to be processed based on the precautionary principle and complemented with a risk-based approach.[16]

The NLF, based on the 'New Approach' to technical harmonisation in product safety law from 1985,[17] was adopted in 2008 to harmonise and improve the way of product safety law making in the EU.[18] Its main goal was to constrain the technical content of legal acts and leave concretisation to European harmonised standards.[19] As this transfers the responsibility of creating technically implementable rulemaking to expert bodies, from a theoretical perspective it promises to improve the quality of technical regulation, legal security and compliance.[20] However, for the price of a lowered degree of democratic legitimacy.[21] Like it is characteristic for product safety law under the NLF, the proposal neither contains substantive individual rights of natural persons whose fundamental rights are affected or could be violated by AI systems nor provides for the possibility of administrative appeal for individuals.[22] Following a concept of risk regulation under the AI Act certain AI practices causing an *unacceptable risk*[23] are prohibited (Art. 5), while AI systems considered to be high-risk (Art. 6) shall follow several material standards and procedural safeguards laid down in Chapter 2 Title III (Art. 8 par. 1).

The GDPR determines obligations of data controllers respectively processors and complementary rights of data subjects in the context of personal data processing as an operation. It intends to strike a balance between collective and individual interests in the processing of personal data and the protection of the rights and interests of data subjects by setting out provisions that leave room for weighing on a case-by-case basis.[24] Theoretically this allows for finding a proportional balance in every individual case, but also requires a certain abstraction of legal provisions which can cause legal uncertainty and difficulties in technical implementability.[25] The legal basis in Art. 6 par. 1 lit. f delivers an example of such a legal norm that can only be applied on a case-by-case basis. Accordingly, a processing of personal data is lawful when it *is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the*

16 Cf. Indra Spiecker gen. Döhmann 'The More the Merier' in Matthias C. Kettemann, Alexander Peukert and Indra Spiecker gen. Döhmann (eds), *The Law of Global Digitality* (Routledge 2022) 77, 87pp.

17 Council Resolution 85/C 136/01 of 7 May 1985 on a new approach to technical harmonization standards <https://eur-lex.europa.eu/EN/legal-content/summary/a-new-approach-to-technical-harmonisation.html> accessed 15 June 2023.

18 Cf. EU COM 'New Legislative Framework' <https://single-market-economy.ec.europa.eu/single-market/goods/new-legislative-framework_en> accessed 15 June 2023; Mark Maynard 'A New Framework for the Eu EMC Directive' (IEEE Symposium on Electromagnetic Compatibility and Signal Integrity, Santa Clara, 15 – 21 March 2015) 7, 7.

19 Council Resolution 85/C 136/01 (n 18); *Mazzini and Scalzo* (n 9) 6; Martin Ebers, 'Standardizing AI: The Case of the European Commission's Proposal for an 'Artificial Intelligence Act' in Larry A. Di Matteo, Cristina Poncibó and Michel Cannarsa (eds), *The Cambridge Handbook of Artificial Intelligence: Global Perspectives on Law and Ethics* (Cambridge University Press 2022) 321, 334 .

20 Cf. Regulation on European standardisation (EU) 1025/2012, Rec. 3; EU COM 'New Legislative Framework' (n 19); with further references regarding the debate on the delegation of regulatory powers to private bodies under EU law, *Ebers* (n 20) 331.

21 With further references *Veale and Zuiderveen Borgesius* (n 6) 105p; *Ebers* (n 20) 339pp.

22 This has been widely criticised, cf. *Smuha and others* (n 6) 44 p; 50 p; *Ebers and others* (n 6) 600; ICCL 'Flaws in ex-post enforcement in the AU Act' [2022] 4p <https://www.iccl.ie/news/flaws-in-ex-post-enforcement-in-the-ai-act/> accessed 15 June 2023. As *Veale and Zuiderveen Borgesius* (n 6) 111 state, also by the EDPB and EDPS Joint Opinion 5/2021 of 18 June 2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (Artficial Intelligence Act) no. 18.

23 COM Proposal AI Act (n 2) Explanatory notes, 5.2.

24 Cf. regarding the need to balance the free movement of personal data with the protection of fundamental rights, Case C-518/07 *Commission v Germany* [2010] OJC 113/3, par. 21pp; and about the need to strike a balance between conflicting fundamental rights in order protect fundamental rights and freedoms of natural persons due to Art. 1 (2), Hilke Hijmans, 'Art. 1 GDPR' in Christopher Kuner and others (eds), *GDPR: A Commentary* (Oxford University Prress 2020) C. 4; more general, *Andrasko, Mesarcik and Hamulak* (n 14) 628.

25 Cf. also Gerrit Hornung and Indra Spiecker gen. Döhmann, 'Einleitung', in: Spiros Simitis, Gerrit Hornung and Indra Spiecker gen. Döhmann (eds), *Datenschutzrecht* [2019] 250pp. A noteworthy current happening is the revision of the case-by-case dependent approach within the Data Protection Law Reform in the UK in the aftermath of Brexit. The proposal for a Data Protection and Digital Information Bill 143 (2022-23) [2] adds in its Sec. 5 par. 4 a new legal basis (Art. 6 lit. ea) that avoids the case-by-case balancing test in response to legal uncertainty caused by its abstractness; for the reasoning see, UK Government, Consultation Outcome Document [23 June 2022] 1.4, https://www.gov.uk/government/consultations/data-a-new-direction/outcome/data-a-new-direction-government-response-to-consultation (accessed 14 June 2023).

interests of fundamental rights and freedoms of the data subject which require protection of personal data. In practice, therefore, the interests in the processing of personal data must be weighed against the conflicting interests in the protection of personal data in each individual case. Further examples for a case-by-case dependency can be found in the GDPR's risk mitigation tools. Certain legal norms rely on a risk assessment that is based on a consideration of each individual case.[26] This can be shown by the controller's obligation to implement *appropriate* technical and organisational measures in Art. 25 par. 1 in order to mitigate the risks of the processing. What measures are appropriate depends inter alia on the *risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing.* Such risks and the likelihood of occurrence must be assessed and weighed by the controller on a case-by-case basis.[27]

In conclusion, the AI Act aims to protect fundamental rights through a technical approach by preventing unacceptable risks in AI systems,[28] while the GDPR determines the relationship between rights and interests in the processing of personal data on the one hand and the protection of personal data on the other hand in legal provisions which often leave room for a case-by-case consideration.

2. Concretisation of the Law

Both the AI Act and the GDPR set out abstract legal requirements. This corresponds to an increased need for flexibility and adaptability in technology law, which must cope with a dynamic and developing subject of regulation.[29] However, a high degree of abstraction in the law creates legal uncertainty and room for maneuver to interpret and apply the law in one's own interest.[30] Thus, concretisation is of high importance to ensure effective application of the law in practice.

a. Harmonised Standards Under the AI Act

The broad and abstract requirements for high-risk AI systems in the AI Act shall be concretised by harmonised standards (Art. 40) or subsidiary common specifications (Art. 41). Considering the subsidiarity of common specifications, the following analysis focuses on harmonised standards. In the face of the presumption of conformity (Art. 40 AI Act) resulting from compliance with standards, these play an essential role in the definition of the requirements high-risk AI systems must comply with.[31] Thus, the legislator has transferred responsibility to standardisation bodies to a large extent.[32] For the development and adoption of technical standards the Regulation on European standardisation (No 1025/2012) applies. On a request of the EU Commission, European standardisation organisations can be mandated to draft a European standard (Art. 10 par. 1). When a draft has been submitted to the EU Commission, it assesses whether the document follows its request (Art. 10 par. 5). If this is the case the EU Commission publishes a reference of the standard in the Official Journal of the European Union (Art. 10 par. 6).

Before the AI Act comes into force, the ESOs will not officially work on the development of harmonised standards. However, they have already been requested to develop 'European Standards' as a basis for following harmonised standards that meet the essential requirements of the AI Act.[33]

For completeness sake it should be mentioned that the EU Commission has been granted several delegated legislative powers to ensure a uniform applica-

26 See also Claudia Quelle 'The Risk Revolution in EU Data Protection Law: We can't have our cake and eat it, too' in Ronald Leenes and others (eds), *Data Protection and Privacy: The Age of Intelligent Machines* (Hart Publishing 2017); *Spiecker gen. Döhmann* 'The More the Merier' (n 17) 88p.

27 Cf. EDPB Guidelines 4/2019 of 20 October 2020 on Article 25 Data Protection by Design and by Default Version 2, 9pp.

28 Critical with regard to the 'overly technocratic approach to the protection of fundamental rights', *Smuha and others* (n 6) 9pp.

29 See also in regard to technology neutrality of the law, Michael Birnhack, 'Privacy Mindset, Technology Mindset' [2014] Jurimetrics 68; *Mitrou* (n 11) 27.

30 Cf. *Quelle* (n 27) 14.

31 *Veale and Zuiderveen Borgesius* (n 6) 104p*; Ebers* (n 20) 338.

32 Cf. *Veale and Zuiderveen Borgesius* (n 6) 105; *Ebers* (n 20) 339p.

33 The AI Act Newsletter 'Standard Setting' <https://artificialintelligenceact.eu/standard-setting/> accessed 15 June 2023. Also there has been some activity in analysing existing standards and current standard activities. In 2020 the Focus Group on AI founded by CEN and CENLEC has published the Road Map on AI that creates an overview of existing standardisation activities concerning AI, cf. StandICT.eu 'CEN-CENLEC Focus Group Report' <https://www.standict.eu/node/4854> accessed 15 June 2023. The European Commission's Knowledge Service called AI Watch analyses existing AI Standards in light of the AI Act, current update: *Soler Garrido and others* 'JRC Technical Report: Artificial Intelligence Standardisation Landscape Update' [2023]; in this regard, Mark Mc Fadden and others, 'Harmonising Artificial Intelligence: The Role of Standards in the EU AI Regulation' Oxford Commission on AI & Good Governance (eds) [2021] 10.

tion and that the law can be adapted to technical developments.[34] But delegated acts under Art. 290 TFEU are intended to be subsequent nonessential legislative additions and therefore not as an application-related concretisation considered here.[35]

b. Concretisation of GDPR Norms

The concretisation of GDPR norms is not based on technical standards, rather on a mix of different concretisation procedures.[36]

Apart from the power to adopt delegated acts (Art. 12 par. 8; Art. 43 par. 8), the EU Commission is also empowered to adopt a variety of implementing acts (Art. 28 par. 7; Art. 40 par. 9; Art. 43 par. 9; Art. 45 par. 3; Art. 46 par. 2 lit. c + d; Art. 47 par. 3; Art. 61 par. 9; Art. 67). While delegated acts are aimed at subsequent nonessential legislative additions, implementing acts are intended to be application-related concretisations.[37]

An important role in the concretisation of the regulation play the European Data Protection Board (EDPB) and the Member State data protection authorities. Under Art. 70 par. 1 the EDPB is assigned the task of providing guidelines, recommendations, and best practices for the consistent application of data protection law in the Union with regard to specific issues, and in lit. e, also by means of a comprehensive general clause. The Board is also competent to issue an opinion on *any matter of general application* under Art. 64 par. 2 on request and non-compliance of a Member State authority with that opinion can initiative the consistency mechanism, at the end of which the EDPB may issue a binding decision. Thus the EDSB has a key function in the concretisation of the law.[38] The Member State authorities also have a range of tasks (Art. 57) that include specification of GDPR norms. Such as the adoption of standard contractual clauses (lit. j), the establishment of a list of processing operations which are subject to the requirement for a data protection impact assessment (lit. k), and the assessment and approval of binding codes of conduct and certification machanisms (lit. m + n).[39] Moreover the tasks of raising public awareness of data protection issues (lit. b) and of making controllers and processors aware of their obligations under data protection law (lit. d) play an essential role in the application-related concretisation of GDPR.[40] In practice the importance of the EDPB and Member State data protection authorities for GDPR concretisation can be seen by the wealth of information available to controllers, processors and data subjects.[41]

In addition to this private actors are included in the concretisation of GDPR norms via procedures of regulated self-regulation. This is particularly the case with an application-oriented specification in procedures for the provision of and compliance with codes of conduct under Art. 40, 41 and the possibility of certification of data processings under Art. 42, 43. However, codes of conduct are to be approved by a data protection authority or the EDPB for Union wide validity (Art. 40 par. 5) and certifications are to be issued by a data protection authority, the EDPB or an accredited certification body (Art. 42 par. 5). Thus, the data protection authorities also play a role in these concretisation procedures.

---

34 Cf. COM Proposal AI Act (n 2) Explanatory Memorandum [5.2.8]. Empowerments to adopt delegated acts can be found in Art. 4; Art. 7; Art. 11 Sec. 3; Art. 43 Sec. 5 + 6; Art. 48 Sec. 5 AI Act.

35 Wolfgang Weiß, 'Dezentrale Agenturen in der EU-Rechtsetzung' [2016] EuR 631, 642pp; Luca Tosoni, 'Art. 92 GDPR' in Christopher Kuner and others (eds), *GDPR: A Commentary* (Oxford University Prress 2020) C.1; Matthias Ruffert, 'Art. 290 AEUV' in Christian Callies and Matthias Ruffert (eds), *EUV/AEUV* [2022] 10pp.

36 For an overview see *Gerrit Hornung and Indra Spiecker gen. Döhmann* (n 26) 250pp.

37 Case C-427/12 *European Commission v Euruopean Parliament and Council of the European Union* [2014] 62012CJ0427, par. 38p; critical in regard to this devision, Jürgen Bast, 'Is There a Hierarchy of Legislative, Delegated and Implementing Acts? [2015] SSRN-Journal <https://ssrn.com/abstract=2645861> accessed 15 June 2023.

38 Orla Lynskey, 'The 'Europeanisation' of Data Protection Law' [2017] 19 Cambridge Yearbook of European Legal Studies 252, 282 speaks of the EDPB as a 'quasi rule-maker', see also in regard to the EDPB's concretisation function, Cornelia Kibler, 'Datenschutzaufsicht im europäischen Verbund: Unabhängigkeit, Effektivität, Rechtsschutz und Legitimation' (Mohr Siebeck 2021) 201pp.

39 Hilke Hijmans, 'Art. 57 GDPR' in Christopher Kuner and others (eds), *GDPR: A Commentary* (Oxford University Prress 2020) C. 5 and 'The European Union as Guardian of Internet Privacy' (2016) 7.4.5 even speaks of 'quasi-legislative activities'.

40 *Hijmans* 'Art. 57 GDPR' (n 40) C. 5 includes these tasks in the category of 'policy- or leadership-oriented tasks' covering a wide range of activities that are not related to classical law enforcement.

41 Cf. the range of guidance, recommendations and practices and opinions available at the webpage of the EDPB <https://edpb.europa.eu/edpb_en> accessed 15 June 2023 and, for example, the information for the public and for organisations on the ICO's webpage <https://ico.org.uk/> accessed 15 June 2023 or of the association of german data protection authorities (DSK) <https://www.datenschutzkonferenz-online.de/> accessed 15 June 2023 .

c. Generalisation vs. Case-by-Case Dependency

As implied by the word standard and explicitly set out in Art. 2 par. 1 Reg. 1025/2012, harmonised standards are intended to provide technical specifications that can be applied repeatedly and continuously. Standardisation of legal provisions in the AI Act is therefore, at least to a certain degree, associated with generalisation on a technical level which aims for improving legal certainty and technical implementability.

In contrast, where GDPR norms rely on a weighing of the conflicting rights and interests in regard to an individual processing operation, no generalisation can be made.[42] The different procedures for concretisation provided for in the GDPR can facilitate its application in practice and can create more legal certainty, but they cannot relieve the applicant of the task of applying the law on a case-by-case basis. In regard to the examples of Art. 6 par. 1 lit. f and Art. 25 par. 1 GDPR this means guidelines on risk assessment published by the EDPB and member state authorities[43] or criteria of certifications and codes of conduct may be instructive as to what should be considered in a balancing test or a risk analysis and assessment, but the responsibility of assessing and weighing remains with the addressee of the legal norm.

In a broader sense, standardisation aims to improve implementability and legal certainty through generalisation on a technical level; while the case-by-case dependent GDPR provisions rely on abstractness to ensure a balance between conflicting rights and interests in every individual case, which in turn hinders their generalisation.[44]

IV. Areas of Tension in the Application

Since the advent of big data technology, the challenges and areas of tension which arise from complex automated mass data processing in relation to data protection law have been discussed.[45] In view of the technical development towards so called Artificial Intelligence, this debate takes on a new significance. There are great hopes of economic and societal benefits following from the use of Artificial Intelligence.[46] On the other hand, there are serious concerns about great risks that AI poses for the fundamental rights and freedoms of the individual and for liberal democratic society.[47] In particular, there are reservations about the compability of AI technologies with fundamental principles of data protection law such as lawfulness, transparency, purpose limitation and data minimisation.[48] With reference to these conflicts between technical conditions of AI and existing data protection law, in the following areas of tension that arise in the application of the AI Act and the GDPR are considered. The analysis herein is based on a model of data accuracy and governance obligations for high-risk AI systems that rely on training with personal data on the one hand and the principle of data minimisation on the other hand.

1. Area of Tension in Concrete Terms – An Example

Even though the regulatory objectives of the AI Act and the GDPR are in line with each other and several regulatory principles like transparency[49], securi-

42 Cf. regarding risk assessment under GDPR Raphaël Gellert, 'The Role of the Risk-Based Approach in the General Data Protection Regulation and in the European Commission's proposed Artficial Intelligence Act: Business as Usual?' [2021] Journal of Ethics and Legal Technologies 16, 22p, who argues that 'calculating risks when fundamental rights are at stake does not lend easily to quantitative and scientific calculations'.

43 Cf. EDSB Guidelines 4/2019 (n 28); Art. 29 Working Party Guidelines of 13 October 2017 on Data Protection Impact Assessment (DPIA) wp 248 rev.01; DSK Kurzpapier Nr. 18 of 26.04.2018 on Risiko für die Rechte und Freiheiten natürlicher Personen.

44 Cf. *Gellert* (n 43) 23; *Smuha and others* (n 6) 12, state that 'The Proposal's requirements erroneousy reduce the careful balancing exercise between fundamental rights to a technocratic process [...]'.

45 Cf. Ira Rubinstein, 'Big Data: The End of Privacy or a New Beginning?' [2012] SSRN Journal <http://www.ssrn.com/abstract=2157659> accessed 15 June 2023; Nikolaus Fargó, Stefanie Hänold and Benjamin Schütze, 'The Principle of Purpose Limitation and Big Data' in Marcelo Corrales, Mark Fenwick and Nikolaus Fargó (eds), *New Technology, Big Data and the Law* (Springer Singapore 2017); Tal Z. Zarsky, 'Incompatible: The GDPR in the Age of Big Data' [2017] Seton Hall L. Rev. 995; Christopher Kuner and others, 'Machine Learning with Personal Data: Is Personal Data Protection Law Smart Enough to Meet the Challenge?' [2017] 7 IDPL, 1.

46 Cf. COM Proposal AI Act (n 2) Explanatory Memorandum [1.1].

47 Cf. COM Proposal AI Act (n 2) Explanatory Memorandum [1.1]; in more detail, Michele Finck and Asia J. Biega, 'Reviving Purpose Limitation and Data Minimisation in Data-Driven Systems' [2021] Technology and Regulation 44, 47; *Jacobs and Simon* (n 8) 13pp.

48 Cf. *Mitrou* (n 11); Christopher Kuner and others, 'Expanding the Artificial Intelligence-Data Protection Debate' [2018] 8 IDPL 289, 290p; *Spiecker gen. Döhmann* 'AI and Data Protection' (n 13) 134 .

49 Art. 13 AI Act (Transparency and provision of information to users) – Art. 5 par. 1 lit. a GDPR (principle of transparency).

ty[50], human oversight[51], and accuracy[52] can be found in both laws; in concrete terms regulatory objectives of the two laws may be in tension with each other and need to be balanced. Such an area of tension may arise between the objective to reach accuracy of a high-risk AI system on the one hand and the objective to keep the amount of personal information processed as low as possible on the other. As an example, a high-risk AI system that is intended to be used for the selection of applicants for a job (AI Act Annex III No. 4 lit. a) and is based on training with personal data is considered herein.

a. Accuracy and Data Governance Obligations Under the AI Act

Art. 15 par. 1 AI Act requires that high-risk AI systems are *designed and developed in such a way that they achieve, in the light of their intended purpose, an appropriate level of accuracy*. Rec. 49 complements this by stating that systems should perform consistently during their lifetimes. Due to Rec. 50 S. 2 they should be resilient against *risks connected to the limitations of the system* such as *errors, faults, inconsistency* and *unexpected situations*, but the recitals do not expressively clarify what is meant with accuracy. According to the general meaning of the word accuracy it is understood in the sense of exactness and correctness.[53] Taking into account the regulatory goal to mitigate the risks for health, safety and fundamental rights[54] and the further explanation from the recitals, for an AI system this refers to the technical functioning and to the output of the system. Therefore, consistent accuracy during the lifetime of an AI system is meant to guarantuee that the system is reliable in its functioning and its output which means it should work free of biases or errors and deviations e.g. caused by noise in the processed data.[55] To achieve accuracy for an AI system, at least if it is a learning system, it might need to be trained with a large amount of high quality data.[56]

The relation between training data and accuracy is captured by more specific rules concerning data governance. For high-risk AI systems which rely on training, Art. 10 AI Act defines quality criteria for training, validation and testing data sets used for the development. Due to par. 3 those data shall be *relevant, representative, free of errors and complete*. The requirement of accuracy and the data governance obligations contain two elements: quality and quantity of data. To achieve accuracy of an AI system, it can not only be important to have a sufficient amount of training data, but also high data quality.[57]

While the requirements 'relevant' and 'free of errors' in Art. 10 Sec. 3 AI Act are clearly related to data quality, 'representative' and 'complete' also concern the quantity of data. As it is explicitly stated in Rec. 44 S. 2 and par. 3 + 4, these criteria must be interpreted on a context-specific basis including the intended purpose of AI systems.

In order to secure an appropriate level of data quality, par. 3 complements that the data shall have *appropriate statistical properties including the persons or group of persons [...] on which the AI system is intended to be used* and par. 4 states that data sets *shall take into account [...] the characteristics or elements that are particular to the specific geographical, behavioural or functional setting* the system is intended to be used in. From this it can be seen that the processing of group- or person-related data which might include personal data or even special categories of personal data protected by Art. 9 GDPR might be required.[58]

In the case of the AI system that is intended to be used for applicant selection, this means in order to achieve accuracy it may need to be trained with a high quantity of personal or even sensitive data as

50 Art. 15 AI Act (Accuracy, robustness and cybersecurity) – Art. 5 par. 1 lit. f GDPR (integrity and confidentiality)

51 Art. 14 AI Act (Human oversight) – Art. 22 GDPR (Automated individual decision-making, including profiling); cf. *Andrasko, Mesarcik and Hamulak* (n 14), 631.

52 Art. 15 AI Act (Accuracy, robustness and cybersecurity) – Art. 5 par. 1 lit. d GDPR. Cf. with regard to the data accuracy principle under GDPR and training data, *Hacker* (n 12) 263.

53 Cf. the description of accuracy in the Cambridge Dictionary 'the fact of being exact or correct' <https://dictionary.cambridge.org/dictionary/english/accuracy> accessed 15 June 2023.

54 Rec. 43 S. 2.

55 D. Petkovic, 'It Is Bot 'Accuracy vs. Explainability' – We Need Both for Trustworty AI Systems' [2023] IEEE Trans. Technol. Soc. 1, 1.

56 cf. Rec. 44 S. 1; *Kuner and others* 'Expanding The Artificial Intelligence-Data Protection Debate' (n 49) 290; *Spiecker gen. Döhmann* 'AI and Data Protection' (n 13) 135; *Petkovic* (n 56) 3p; with further references Pablo Trigo Kramcsák, 'Can legitimate interest be an appropriate lawful basis for processing Artificial Intelligence training datasets?' Computer Law & Security Review [2023] 105765, 3 f; with regard to the dangers following from insufficient data management and data preparation, *Jacobs and Simon* (n 8) 14pp.

57 Cf. Rec. 44 S. 1 AI Act; *Finck and Biega* (n 48) 45p; *Petkovic* (n 56) 3.

58 Cf. the examples of biases in image recognition AI systems or those used in hiring processes, *Jacobs and Simon* (n 8) 15p.

long as they are relevant for a decision between applicants in the respective sector.

b. Data Minimisation Under GDPR

Art. 5 par. 1 lit. c GDPR states that personal data processed *shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed*. The principle of data minimisation is closely linked to the principle of purpose limitation of Art. 5 par. 1 lit. b GDPR which requires purpose specification and the bond of processing to that purpose.[59] Adequacy, relevance and necessity in Art. 5 par. 1 lit. c GDPR relate to the specified purpose of processing. The processing of inadequate or irrelevant data that is not suitable and pertinent in relation to it would breach the data minimisation principle.[60] The criterion of necessity is stricter compared to the GDPR's predecessor the Data Protection Directive (DPD), which only required that the data processed must not be *excessive in relation to the purposes*.[61] The GDPR principle requires a test regarding any processed data whether it is necessary for achieving the defined purpose. In negative terms, this means the data minimisation principle hinders the processing of data if the purpose can be achieved without. Likewise the accuracy requirements under the AI Act, the principle refers to data quantity as well as to data quality.[62] This means that the amount of personal data processed should be kept as low as possible, taking into account the purpose of processing.[63] In addition, the intrusiveness of data quality should be kept as low as possible which means special categories of personal data should only be processed if other data that are not covered by Art. 9 GDPR are not sufficient to achieve the purpose of processing. As stated by the ICO, only the 'minimum amount of information' needed should be processed, and the need is to be determined separately for each individual or group of individuals sharing relevant characteristics.[64] For the applicant selection AI system, therefore, only as much personal data as necessary to fulfil the training purpose should be processed and the proportion of special category of personal data must be kept as low as possible.

The principle of data minimisation is manifested in numerous more specific GDPR norms. For instance, all legal bases in Art. 6 par. 1 lit.b – f require that the processing is necessary for the respective purpose or the right of erasure if personal data are no longer necessary for the purpose of its processing from Art. 17 par. 1 lit. b.[65] Hence, where there is an area of tension between the obligations of the AI Act and the data minimisation principle, this also has an effect with regard to connected principles like lawfulness, purpose limitation and storage limitation as well as other GDPR requirements that concreticise these principles.

c. Conflicting Obligations and Their Relation

Partly, the requirement of accuracy under Art. 15 AI Act might go hand in hand with the GDPR principle of data minimisation. But, they can also be in tension with each other.[66] In order to achieve accuracy of an AI system that is based on training, the respective importance of data quantity and quality depends on the specific technique used in the AI system and the purpose it is intended to be used for. In some cases a reduction of data quantity or quality might even improve the accuracy of the system.[67] From this it becomes clear that, in view of the multiplicity, complexity and opacity of the subject matter, AI regulation and Data Protection law do not conflict in gen-

59 Regarding the purpose limitation principle, *Spiecker gen. Döhmann* 'AI and Data Protection' (n 13) 135.

60 *Finck and Biega* (n 48) 56.

61 Art. 6 par. 1 lit. c Directive 95/46/EC; Cécile de Terwangne, 'Art. 5 GDPR' in Christopher Kuner and others (eds), *GDPR: A Commentary* (Oxford University Prress 2020) C. 3; *Finck and Biega* (n 48) 56.

62 *Cécile de Terwangne* (n 62) C. 3; *Finck and Biega* (n 48) 56p; cf. also *Zarsky* (n 46) 1011.

63 *Finck and Biega* (n 48) *56,* argue in regard to algorithmic profiling, personalisation and decision-making systems that it can follow from the principle of adequacy that more personal data should be processed if this seems appropriate for the pursuit of the overall purpose considering other GDPR principles such as fairness, transparency and accuracy. However, considering that GDPR applies to data processing, the data minisation principle refers to a specified data processing operation. Thus, adequacy must be assessed in relation to the data processed in that operation and in relation to its specified purpose, but not in relation to data that could potentially be processed and not to the overall purpose from the point of view of a controller or processor. Any conflicts with other GDPR principles are to be resolved by weighing them on a case-by-case basis.

64 ICO, A Guide to the Data Protection Principles, Data minimisation, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/> accessed 15 June 2023.

65 Cf. also *Mitrou* (n 11) 49pp. The data protection principles are a basis for the interpretation of more specific GDPR norms, *Spiecker gen. Döhmann* 'AI and Data Protection' (n 13) 134.

66 See also, *Kramcsák* (n 57).

67 Cf. *Finck and Biega* (n 48) 45p.

eral. Rather areas of tension need to be determined with regard to certain legal provisions and concrete processing operations taking into account their purposes and means.

In the following we consider the case where more high quality training data enhances the accuracy of the applicant selection AI system. Due to the data minimisation principle the question arises if personal data that is used or planned to be used for the training of the AI system is adequate, relevant and necessary. As data protection law applies to a specific processing operation or a set of operations and not to a product or a software as a whole,[68] this must be considered separately for any data revealing information about an individual. Taking into account the objective of the principle to restrict the amount and intrusiveness of personal data processed, the conflict with the accuracy and data governance obligations that require the processing of a huge amount of high quality data becomes evident.[69]

However, adequacy, relevance, and necessity must be determined depending on the purpose of the processing. The purpose of the processing in the example considered here is the training of the AI system that is intended to be used for the selection of applicants. Hence, the question arises what amount and type of data is needed for a successful training.[70] The relation to the purpose of processing in the data minimisation principle thus becomes a gateway for AI-specific considerations that focus on the system as a whole rather than on a single processing operation. From that viewpoint, the training can be considered successful if it contributes to a reliable and persistent functioning of the system which means its output should be meaningful and informative for the employer as well as fair, especially non-discriminatory, towards the applicants. This meets the requirement of accuracy under the AI Act which pursues to mitigate the risks for health, safety and fundamental rights of natural persons.[71] It is also in line with the main objective of data protection law to the extent it is aimed at protecting (other) fundamental rights and freedoms, such as freedom of non-discrimination.[72] However, at the same time it challenges the goal of restricting the amount and intrusiveness of personal data processed in order to protect the right to data protection.

Legal provisions regarding the quantity and quality of training data sets required for a successful training are in turn set out in Art. 10 AI Act. As complementary law, the AI Act contains more specific rules concerning AI systems, which apply in addition to the GDPR without restraining the latter. From this and in the sense of consistency of the Union legal system, it follows that if the purpose of the processing is the training of a high-risk AI system then the requirements of adequacy, relevance and necessity of Art. 5 par. 1 lit. c GDPR that are related to the purpose, must be interpreted and applied with respect to the provisions of Art. 15 and Art. 10 AI Act. Hence, the assessment of what amount and type of data are adequate, relevant and necessary for the purpose of the training of a particular AI system must be measured according to the criteria of relevance, representativeness, freedom of errors and completeness under Art. 10 par. 3 AI Act and in order to achieve accuracy due to Art. 15 par. 1 AI Act. At the same time the GDPR remains unaffected by the AI Act. Thus, the requirements of accuracy and data governance must be interpreted with respect to the data minimisation principle and its main objective to restrict the personal data processed to the minimum amount and intrusiveness. Consequently, both the data minimisation principle under Art. 5 lit. c GDPR and the obligations on accuracy and data governance under the AI Act must be interpreted and applied in accordance with their respective regulatory objective, but also with consideration of each other. Where there are areas of tension, a balance must be struck.

2. Balancing of Conflicting Regulatory Goals

As already shown, the AI Act and the GDPR may apply parallel to providers and users of AI systems in practice. Therefore, to facilitate a coherent interpretation and thus an effective application of both legal acts, where conflicting obligations must be balanced, there is a need for substantive legal provisions that

68 Art. 2 par. 1; Art. 4 par. 2 GDPR.

69 *Mitrou* (n 11) 50, states that 'the principle of data minimisation is – almost by definition – opposed to Big data analytics and machine learning systems that are based, if not dependent on an excessive data collection […]'.

70 From a technical viewpoint that cannot be exactly defined, *Liza* (n 16) 4.

71 Cf. Rec. 43 S. 2 AI Act.

72 Cf. Art. 1 par. 2 GDPR; Rec. 4, 75 GDPR.

set the parameters of weighing or at least for procedural safeguards that secure a coordinated concretisation of the conflicting laws.

a. Substantive legal provisions

The AI Act only contains a few substantive requirements as to how conflicting regulatory goals and the resulting obligations between AI Act and GDPR are balanced.[73] Even if it is typical for legal acts under the NLF, that specification is left to standardisation bodies to a large extent,[74] it should be considered that such questions of balancing between data protection law and AI regulation are essential matters that affect the protection of fundamental rights. The case of the applicant selection AI system illustrates this clearly. Regulatory goals are in tension with each other, where the processing of personal data restricted to a minimum is beneficial to the fundamental right to data protection (Art. 8 CFR), but a particularly extensive data processing serves the accuracy of the system and thus the protection of other fundamental rights such as the freedom to conduct a business (Art. 16 CFR) of the provider and user of the AI system, and the freedom to chose an occupation (Art. 15 CFR) as well as the right to non-discrimination (Art. 21 CFR) of the applicants.

In regard to the processing of special categories of personal data, that could help prevent discriminatory biases,[75] the AI Act specifies the relationship of the data minimisation principle and the data governance obligations. Art. 10 par. 5 AI Act creates a legal basis for the processing of special categories of personal data to the extent that it is strictly necessary for the purposes of ensuring bias monitoring, detection and correction. This is supplemented by the obligation of the provider to implement appropriate safeguards like pseudonymisation or encryption.[76] Although the questions of what is strictly necessary and what measures are appropriate remain; the definition of the purpose, the emphasis on strict necessity, and the obligation to implement risk mitigating measures specify the relation between the conflicting fundamental rights. The right to data protection must take a secondary place to the right of non-discrimination, if the processing of special category data is strictly necessary to avoid biases.[77] The former must be protected as far as possible by additional measures.

However, apart from the processing of special categories of personal data to avoid biases it remains unclear to what extent the right to data protection should be restricted in order to ensure the most accurate output of the system and thus take into account other fundamental rights such as the freedom to conduct a business and the freedom to chose an occupation.[78]

Moreover, if the processing is to be based on Art. 6 par. 1 lit. f GDPR,[79] a balancing test between the *legitimate interest* in the processing *pursued by the controller or a third party* and the interest in the *protection of fundamental rights and freedoms of the data subject that require protection of personal data* must be carried out. In this case the law does not provide any further information for weighing the legitimate interest to reach accuracy of the AI system and the interest in restricting the amount of information processed and the fundamental rights behind it.

That the AI Act lacks sufficiently concrete substantive provisions on matters relevant to fundamental rights has already been widely critised with respect to democratic inadequacies of the standardisation procedures.[80] This is particularly true in areas where legal norms protecting fundamental rights conflict each other. Thus, in areas of tension between GDPR norms and obligations under the AI Act there is need for a substantive balancing in the law.

b. Coordinated Conretisation

Where the law does not contain any substantive requirements for balancing conflicting obligations, its

73 Rec. 72 – legal basis for regulatory sandboxes; Art. 10 (5). Also criticising the lack of clearance regarding the relationship between the GDPR and the AI Act and in concrete terms between data governance obligations and GDPR, *Smuha and others* (n 6) 34, 41pp.

74 See above under III. 1.

75 Cf. Rec. 44 S. 6; Marvin van Bekkum and Frederik Zuiderveen Borgesius, 'Using Sensitive Sata To Prevent Discrimination by Artificial Intelligence: Does the GDPR Need a New Exception [2023] 48 Computer Law & Security Review 105770, 105773.

76 Critial in terms of the limited scope of the legal basis that only applies to high-risk AI systems, *Veale and Zuiderveen Borgesius* (n 6) 103.

77 Whereby here, too, the specified purpose remains vague. As *Ebers and others* (n 6) 569 state, it is not clarified by the AI Act what forms of biases are covered.

78 Also arguing in this direction, *Hacker* (n 12) 297f.

79 See in regard to lit. f as a legal basis for data processing by an AI system, *Spiecker gen. Döhmann* 'AI and Data Protection' (n 13) 139p.

80 Cf. *Ebers* (n 20) 343. Generally the standardisation process under the NLF has been critised for structural defictis for long before, cf. with further references, ibid. p. 339; *Veale and Zuiderveen Borgesius* (n 6) 105; *Smuha and others* (n 6) 54.

concretisation is of central importance for a coherent and effective application. This applies in particular to the case considered here where proivisions of different legal acts come together in practice and have to be reconciled with each other. It should be concretised for providers of AI systems how the accuracy and data governance obligations are to be interpreted taking into account the data minimisation principle, and respective to controllers in the sense of GDPR in the reverse case.

i. Lack of Consistency in the Concretisation of the AI Act and the GDPR

As described under III., the AI Act and the GDPR pursue different concepts of legal concretisation. While the requirements for high-risk systems from Title III Chapter 2 of the AI Act are to be specified by clear and technically implementable standards; the provisions of the GDPR, which are open to interpretation on a case-by-case basis, are concretised in different procedures, whereby a responsibility of interpretation and application in the individual case remains with the controller or processor.

Harmonised standards are developed by mandated private institutions, the European Standard Organisations (ESOs), listed in Annex I of Regulation 1025/2012.[81] The ESOs are obliged under Art. 5 Reg. 1025/2012 to encourage and facilitate an appropriate representation and participation of all relevant stakeholders (par. 1) and, in standardisation activities concerning an emerging area with significant political or technical innovation implications, of scientific entities at technical level (par. 2). However, this is mainly left to internal regulations of the standardisation organisations. There are neither more concrete duties nor a control mechanism or sanctions that would safeguard the effective involvement of stakeholders,[82] and in practice the stakeholder involvement is criticised as insufficient.[83] At national level, due to Art. 7 Reg. 1025/2012, member states shall encourage the participation of public authorities in national standardisation activities aimed at the development or revision of EU standards, but there is no obligation or encouragement for the ESOs to involve EU bodies or authorities whose area of responsibility is affected by the standardisation activity.

Considering the example made here, the standardisation organisation must define technical standards ensuring that AI systems operate accurately in the sense of Art. 15 par. 1 AI Act and that data processed is relevant, representative, free of errors, and complete in accordance with Art. 10 par. 3 AI Act. In the interest of a coherent and effective application of the AI Act and the GDPR, due to the data minimisation principle under Art. 5 lit. c GDPR this must be determined taking into account what is appropriate, relevant, and necessary for the specified purpose of processing. The latter might in turn be specified on a European level by guidelines, recommendations, best practices, or opinions of the EDPB, and by approved codes of conduct or certification criteria. However, neither the ESOs nor the EDPB are obliged or encouraged by the law to consult the other actor or involve it in the development of their standards respecticely their guidelines etc..

For completeness sake it is to be noted that the European Data Protection Supervisor is represented in the European Artificial Intelligence Board (Art. 57 par. 1 S. 1 AI Act) and that exchanges with other Union bodies, as the EDPB is one, shall be facilitated by the EU Commission (par. 4 S. 2). Nevertheless, the European Artificial Intelligence Board is only responsible for opinions regarding standardisations and their application (Art. 68 lit. c (i) + (ii) AI Act) and has no active participation in standardisation activities or even an approval function. Due to Art. 10 par. 5 Reg 1025/2012 only the approval of the EU Commission is required and even the Commission's assessment power is limited to formal aspects.[84]

The lack of coordination of the concretisation procedures can lead to the fact that areas of tension, which exist between the legal provisions of the AI Act and the GDPR, are perpetuated in the respective standards or guidelines etc., so that these do not contribute to a coherent application of both regulations in practice. Consequently, there is a need for procedural safeguards to coordinate the concretisation procedures. Considering that the AI Act is the more specific law and that the Reg. 1025/2012 applies subsidiary for standardisation procedures, an obligation or procedure for the ESOs to involve the EDPB in

81 These are CEN (European Committee for Standardisation); CENELEC (Europan Committee for Electrotechnical Standardisation) and ETSI (European Telecommunications Standards Institute).

82 *Ebers* (n 20) 341.

83 *Mc Fadden and others* (n 34) 20p; *Veale and Zuiderveen Borgesius* (n 6) 105; *Ebers* (n 20) 341 .

84 *Ebers* (n 20), 340.

their standardisation activities could be provided for there. However, with regard to any coordination of the procedures it should be mentioned that the complete independence of the EDSB sets a rigid boundary.

ii. Challenges of a Coherent Concretisation

The concretisation of legal provisions of the AI Act in consideration with conflicting GDPR requirements encounters difficulties that are related to the differences in the regulatory concepts of the two legal acts.

Generally, reasonable doubts are raised with regard to the formulation of broadly applicable and clearly defined standards for highly complex technical systems that are subject to constant development, and whose risks depend significantly on the purposes and contexts for which and in which they are intended to be used.[85] Furthermore it remains to be determinded whether and how the ESOs should and can deal with normative and ethical questions associated with standard setting for AI.[86] This becomes particularly clear with regard to the consideration of transferring GDPR provisions into standards. As it has been pointed out under III.2.c the case-by-case dependency of GDPR provisions hinders the generalisation technical standardisation aims for. Where GDPR requirements are in tension with those of the AI Act, and fundamental rights must be weighed to strike a balance between them, the law can only be concreticised insofar as criteria (potentially) relevant for the weighing and its parameters are defined. The weighing as such must always be context-dependent, which means it remains to the interpretation and application in the concrete individual case. An example for this can be found in the balancing of the right to data protection and the right to non-discrimination due to Art. 10 Sec. 5 AI Act as already mentioned before. Thus, the transferability of the relation between conflicting legal provisions under the GDPR and the AI Act into clear technical standards is challenging because of significant differences between the chosen regulatory approaches. A coordination of the different concretisation procedures requires coordination of these different approaches in the first place. This means a bridge must be built between generalisation on a technical level for the sake of implementability and legal certainity on the one hand, and case-by-case-dependency aiming for a proportional balance in every individual case on the other. As proportionality is an indisputable principle of EU primary law and GDPR should remain unaffected by the AI Act, it may be required to compromise on the level of generalisation that can be reached by harmonised standards.

VI. Conclusion and Outlook

The Commission's proposal for an AI Act and the GDPR pursue similar regulatory objectives from an overall-viewpoint, but the regulatory goals conflict in concrete terms. In view of the overlapping areas of application, legal provisions must be interpreted and applied with consideration of each other. Although this is an essential matter concerning the protection of fundamental rights the Commission's proposal does not sufficiently address it. There is a need for substantive provisions to balance Data Protection Law and AI Regulation or at least for procedural safeguards that ensure a coordinated concretisation of both laws in order to secure their coherent and thus effective interpretation and application. As GDPR provisions, whose application requires a weighing of fundamental rights on case-by-case basis, cannot be generalised, it remains questionable to what extent it will be possible to generalise the legal provisions of the AI Act through harmonised standards while taking conflicting GDPR provisions into account.

85 *Ebers* (n 20) 332; *Mc Fadden* and others (n 34) 19, do not doubt that, but admit that it will be challenging that standards 'need to be sufficiently flexible to address a wide range of use case risks'. Regarding the data governance obligations under Art. 10 par. 3; *Ebers and others* (n 6) 595, state that they are 'technical not feasible'. In regard to the data governance obligations under Art. 10 par. 5 AI Act Maria-Camilla Fiazza, 'The EU Proposal for Regulating AI: Foreseeable Impact on Medical Robotics' (IEEE 20th International Conference on Advanced Robotics (ICAR), Ljubljana, December 2021) 222, 223p points out that from a technical perspective it remains unclear how to apply to it. Following on from this, *Liza* (n 16) 4, argues that the necessary level of data quantity cannot be generalised.

86 Cf. Johann Laux, Sandra Wachter and Brent Mittelstadt, who propose a development of standards that require 'ethical disclosure by default' by the ESOs ,'Three Pathways for Standardisation and Ethical Disclosure by Default under the European Union Artificial Intelligence Act' [2023] SSRN Journal <https://ssrn.com/abstract=4365079> accessed 15 June 2023.