PART IX

The AI Act Interactions with the Digital Rulebook

34

The AI Act and the GDPR

GLORIA GONZÁLEZ FUSTER

The Artificial Intelligence Act (AI Act)[1] is connected to the General Data Protection Regulation (GDPR)[2] in several significant ways. Some of these connections appear to hint towards a convergence (be it the partial concomitance of their goals, the presence of some shared notions, the reliance on some similar mechanisms), whereas others are rather divergences, or point at least towards a clear separation, as well as a recurrent distancing. The overall picture drawn by the AI Act and the GDPR might look like a series of intersecting zigzagging lines and *trompe l'oeil* resemblances, potentially inducing some confusion. This contribution offers a series of pointers to better understand what exactly is at stake in this not straightforward – but crucial – relationship.

The AI Act cannot, in any case, be fully understood or applied ignoring the GDPR: some AI Act rules build directly and expressly on possibilities introduced in EU law by the GDPR, modulating its legal effects. As a consequence, this also implies that nowadays, to completely apprehend the legal significance of the GDPR, it is essential to be aware of what the AI Act does to it.

This contribution first situates the overall dynamics of the relationship between the AI Act and the EU's data protection law *acquis* in general, of which the GDPR is an important component, but not the only one. Second, it examines some of the specific interplays and intersections between the AI Act and the GDPR. This overview cannot by itself alleviate all uncertainty surrounding these two important EU acts, but it aims at preventing some possible basic misconceptions and at identifying as narrowly as possible remaining knowledge gaps.

34.1. The AI Act and EU Data Protection Law

The AI Act aims to regulate AI systems without directly interfering with the EU personal data protection *acquis*. This *acquis* is epitomised by EU primary and secondary law: EU primary law as in Article 8 of the EU Charter of Fundamental Rights and Article 16 of the Treaty on the

[1] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance), OJ L, 2024/1689, 12.7.2024.

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), OJ L 119, 4.5.2016, pp 1–88.

Functioning of the EU (TFEU), both enshrining the EU fundamental right to personal data protection,[3] and secondary law including the GDPR[4] but also the so-called 'Law Enforcement' Data Protection Directive (LED),[5] and Regulation (EU) 2018/1725 (EU DPR),[6] as well as the 'e-Privacy Directive'.[7]

The AI Act notes that personal data shall be processed in the context of the rights and obligations it establishes. When this occurs, EU personal data protection law shall apply, and must therefore be complied with. The AI Act's guiding principle, formulated in its Article 2(7), is, in this sense, that it does 'not affect' EU data protection law. Recital 10 AI Act stresses the same principle: the AI Act 'does not seek to affect the application of existing' EU data protection law. Article 2(7) AI Act adds, however, that this 'not affecting EU data protection law' is only true 'without prejudice to' two AI Act provisions: Articles 10(5) and 59 AI Act. This nuance might be interpreted as conceding that, to some extent, and at least insofar as these two provisions are concerned, the AI Act does *affect* EU data protection law.

The cardinal principle of not affecting or not interfering with EU data protection law coexists thus with a subtle concession of some possible impact. The principle, in any case, should not be read as signifying that the AI Act is generally unconcerned with personal data protection, the insurance of which is actually one of its objectives. All these somehow overlapping dynamics deserve some contextualisation.

34.1.1. AI Act and GDPR, Same Fight

Perhaps the most significant connection between the AI Act and EU's personal data protection is that the AI Act aims to improve the EU's internal market's functioning, to support innovation, and to protect against the harmful effects of AI systems while ensuring a high level of protection of health, safety, and the 'fundamental rights as enshrined in the Charter of Fundamental Rights of the European Union (the "Charter")'.[8] Considering that the fundamental right to personal data protection is one of such fundamental rights enshrined in the Charter, ensuring a high level of personal data protection logically constitutes one of the very aims of the AI Act.

[3] On this right, see: G González Fuster, *The emergence of personal data protection as a fundamental right of the EU* (Springer, 2014).

[4] On the GDPR, see notably: C Kuner, LA Bygrave and C Docksey (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press, 2020).

[5] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016, pp 89–131. On this Directive, see notably: E Kosta and F Boehm (eds), *The EU Law Enforcement Directive (LED): A Commentary* (Oxford University Press, 2024).

[6] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, OJ L 295, 21.11.2018, pp 39–98.

[7] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002, pp 37–47, as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, OJ L 337, 18.12.2009, pp 11–36.

[8] Recital 1 of the AI Act. See also, in the same sense, Recital 8.

As a matter of fact, references in the AI Act to the imperative of developing the AI regulatory framework in accordance with EU fundamental rights mention not only the fundamental rights recognised in the Charter, but also those enshrined by the EU Treaties[9] – and the right to personal data protection is actually also recognised in the Treaties (Article 16(1) TFEU). On top of that, ensuring a high level of protection of public interests as regards to fundamental rights is described as requiring guaranteeing consistency not only with the Charter, but as demanding also to take into account the European Declaration on Digital Rights and Principles for the Digital Decade.[10] This Declaration additionally asserts that everyone has the right to the protection of their personal data.[11] In sum, guaranteeing a high level of personal data protection is thus an integral part of the objectives of the AI Act in more ways than one.

The AI Act highlights possible encroachments with EU fundamental rights – and particularly possible encroachments with the EU fundamental right to data protection – to justify some of its key policy choices.[12] It notably refers to the fact that the 'extent of the adverse impact caused by the AI system on the fundamental rights protected by the Charter is of particular relevance when classifying an AI system as high risk', adding that those rights include the right to protection of personal data.[13] Furthermore, it argues that 'novel and powerful tools for manipulative, exploitative and social control' 'should be prohibited because they contradict Union values' such as the respect for the fundamental rights enshrined in the Charter, including the rights 'to data protection and to privacy'.[14] Similarly, the AI Act points out that AI systems used to monitor the performance and behaviour of persons in work-related contractual relationships may 'undermine their fundamental rights to data protection and privacy'.[15]

Personal data processing appears not only as such a general concern. By virtue of Article 7 AI Act, the European Commission is empowered to amend Annex III by adding or modifying use-cases of high-risk AI systems, and it shall do so taking into account the adverse impact of the AI systems at stake on fundamental rights. When carrying out this assessment of a potential 'adverse impact', the European Commission must notably take into consideration the 'nature and amount of the data processed and used by the AI system, in particular whether special categories of personal data are processed'.[16]

Because of its fundamental rights nature, EU personal data protection matters also for determining the applicability of certain AI Act provisions. In this regard, Article 6(3) AI Act exempts from being considered a high-risk AI system the systems that, despite being referred to in Annex III AI Act,[17] do not 'pose a significant risk of harm to the health, safety or fundamental rights of natural persons, including by not materially influencing the outcome of decision making'. Recital 53 AI Act comments on this criterion by putting forward a limit to such an exception, a limit which is connected to data protection law. The Recital observes indeed that

[9] *cf* for instance Recital 6 of the AI Act.

[10] See Recital 7 of the AI Act.

[11] See point 17 of the European Declaration on Digital Rights and Principles for the Digital Decade (OJ C 23, 23.1.2023, pp 1–7).

[12] Similar references are also to be found, for instance, in the European Commission's *Guidelines on prohibited artificial intelligence practices* (European Commission, Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act), Brussels, 29.7.2025, C(2025) 5052 final: see for instance para 137).

[13] Recital 48 AI Act.

[14] Recital 28 AI Act.

[15] Recital 57 AI Act.

[16] Article 7(2)(c) AI Act.

[17] Annex III AI Act is titled 'High-risk AI systems referred to in Article 6(2)'.

in any case AI systems used in high-risk use-cases listed in Annex III 'should be considered to pose significant risks of harm to the health, safety or fundamental rights if the AI system implies profiling within the meaning of' Article 4(4) GDPR, Article 3(4) LED, or Article 3(5) EU DPR – making thus directly relevant for the qualification of an AI system as a high-risk AI system the applicability of specific provisions (on profiling) of EU's personal data protection *aquis*.

34.1.2. It's about the NLF, Simply

The AI Act builds on the EU's legal instruments constituting the New Legislative Framework (NLF), instruments which insist on the idea that they are 'without prejudice' to existing EU law and any possibly existing obligations of relevant actors.[18] As a matter of fact, the NLF not only formally respects EU fundamental rights, but 'seeks to ensure full respect' for rights and principles such as consumer protection or the protection of personal data.[19] Consistent with this approach, Recital 9 of the AI Act notes that the AI Act, 'in line with the New Legislative Framework, should be without prejudice to existing' EU law, 'in particular on data protection'. Recital 157 similarly highlights that the AI Act is 'without prejudice to the competences, tasks, powers and independence of relevant national public authorities or bodies which supervise the application' of EU law, including data protection authorities.

Occasionally, the AI Act makes an additional explicit reference to the fact that it shall not alter the applicability of any other possibly applicable EU laws. This is the case, for instance, in Article 5(8), which states that the prohibitions under the AI Act 'shall not affect the prohibitions that apply where an AI practice infringes other Union law'. Although data protection law is not mentioned here, data protection law might have been on the mind of the legislator in this particular regard. Data protection law is, in this sense, mentioned in Recital 45, which proclaims that '(p)ractices that are prohibited by Union law, including data protection law, (…) should not be affected' by the AI Act.

In a similar vein, Recital 63 of the AI Act observes that the fact that an AI system would be classified by the AI Act as a high-risk AI system 'should not be interpreted as indicating that the use of the system is lawful under other acts' of EU or national law, 'such as on the protection of personal data'. It then adds that any use of such AI systems must occur 'in accordance with the applicable requirements resulting from the Charter and from the applicable acts of secondary Union law and national law'.[20] Illustrating the same phenomenon, Recital 95 stresses that post-remote biometric identification systems should be subject to safeguards '(w)ithout prejudice to applicable Union law, in particular Regulation (EU) 2016/679 and Directive (EU) 2016/680'.

It is thus the AI Act's anchorage in the NLF that explains its emphasis on not affecting the EU's data protection law *acquis*, while pursuing, just like all the instruments of such *acquis*, the protection of fundamental rights – including the right to data protection.

[18] See, for instance, Recital 12 of Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011: 'This Regulation should be without prejudice to the obligations corresponding to the roles of each of the economic operators in the supply and distribution process pursuant to specific provisions in Union harmonisation legislation'.

[19] See Recital 68 of Regulation (EU) 2019/1020.

[20] Recital 63 AI Act.

34.1.3. Echoes of Ethics

An additional link between the AI Act and data protection – perhaps the most convoluted of them all – is visible in its Recital 27, a throwback to the 2019 Ethics guidelines for trustworthy AI of the AI High-level Expert Group (HLEG),[21] a non-binding document predating the EU's decision to legislate on AI.[22] The Recital celebrates the ethical principles put forward by those Guidelines, noting nevertheless that such ethical principles are '(w)ithout prejudice' to the legally binding requirements of the AI Act itself 'or any other applicable law'. The Recital then goes on to describe the '(p)rivacy and data governance' ethical principle presented in the Guidelines as meaning that AI systems must be developed and used 'in accordance with privacy and data protection rules' – a statement which is certainly true, but of limited added value, as applicable data protection law is, and will be, applicable regardless of the existence of any ethical principle in a non-binding document hinting it is ethically sound to respect applicable law. Further adding to the conceptual fuzziness of these reflections, the Recital concludes by inviting all stakeholders to 'take into account, as appropriate, the ethical principles for the development of voluntary best practices and standards' – as if taking into account the obligation to comply with the law was a choice that one may or may not take into account when developing best practices.

All in all, the commented passage in Recital 27 does little to bring clarity on the exact relationship between the AI Act and data protection law, trapped in the HLEG's legacy of imprecision.

34.1.4. The AI Act as Partially Data Protection Law

The AI Act is not just related to the EU's data protection law *aquis*, as a pre-existing and external set of rules. The AI Act is actually itself, in part, data protection law. Significant elements of the AI Act have indeed as a legal basis Article 16 of the TFEU, a primary law provision stating since 2009 that the European Parliament and the Council shall lay down the rules relating to the protection of individuals with regard to the processing of personal data, as well as the rules relating to the free movement of such data.

The other legal basis on which the AI Act relies – and on which are based most of its provisions – is Article 114 TFEU, concerning the establishment and functioning of the internal market. The choice of 114 TFEU is consistent with the purpose of the AI Act as presented in Recital 1, which explicitly refers to the improvement of the functioning of the internal market.[23]

The reason why some elements of the AI Act needed to be based on a legal basis different from Article 114 TFEU is not explained in the AI Act. Its Recital 3 simply introduces as a fact that '(t)o the extent that' the AI Act 'contains specific rules on the protection of individuals with regard to the processing of personal data concerning' certain restrictions of uses of AI systems, 'it is appropriate to base [the AI Act], in so far as those specific rules are concerned, on Article 16 TFEU'. Concretely, these provisions to be based on Article 16 TFEU are those about 'restrictions

[21] Also mentioned in Recital 7 of the AI Act.

[22] On the blurred boundaries between ethics and law as perceived by the HLEG, see: G González Fuster (2020), *Artificial Intelligence and Law Enforcement: Impact on Fundamental Rights*, European Parliament, Policy Department for Citizen's Rights and Constitutional Affairs, Directorate-General for Internal Policies PE 656.295 July 2020, p 54 ff.

[23] The idea is also further developed in Article 3 AI Act.

of the use of AI systems for remote biometric identification for the purpose of law enforcement', those on restrictions of 'the use of AI systems for risk assessments of natural persons for the purpose of law enforcement', and those on restrictions of 'the use of AI systems of biometric categorisation for the purpose of law enforcement'.

The common denominator of all these AI Act rules based on Article 16 of the TFEU is, thus, that they relate to law enforcement, and could thus not be based on Article 114. The rationale behind the choice appears to be, therefore, basically that Article 114 was not a realistic choice for these provisions, because, being about law enforcement, they are not about the functioning of the internal market. The possibility of relying on Article 114 had to be eliminated, and there might actually be no naturally appropriate, manifestly adequate legal basis in the Treaties for the EU legislator to generally decide on what the police can do with AI in the EU. The reliance on 16 TFEU could thus be described as a creative solution for the specific problem of a lack of a better legal basis in EU law. Its real suitability might be questioned. In this sense, for instance, if basing the restrictions on the use of AI systems of biometric categorisation for the purpose of law enforcement in Article 16 TFEU was a meaningful choice, it is unclear why it should not have been appropriate to also base in Article 16 TFEU all other restrictions on the use of AI systems.[24]

Among the three sets of AI Act rules which have been based on Article 16 TFEU, one is partially placed in a particular legal position: the restrictions of the use of AI systems for remote biometric identification for the purpose of law enforcement, but more specifically the rules that prohibit the use of AI systems for real-time remote biometric identification of natural persons in publicly accessible spaces for the purpose of law enforcement subject to certain exceptions, 'should apply *as lex specialis* in respect of the rules on the processing of biometric data contained in Article 10 of Directive (EU) 2016/680'.[25] No explanation is provided as to why only these provisions apply as *lex specialis* in respect to the LED. Recital 38 AI Act hints at the fact that this must be so because remote biometric identification involves the processing of personal data, but biometric categorisation also involves the processing of personal data, and these provisions are not framed as *lex specialis* with respect to the LED.[26]

In any case, the consequence of this specification would be, according to Recital 38 AI Act, that the processing of biometric data in the context of the use of AI systems for real-time remote biometric identification of natural persons in publicly accessible spaces for the purpose of law enforcement must comply directly with the AI Act,[27] while the relevant competent authorities

[24] Also raising questions about the use of Article 16 TFEU as (partial) legal basis, emphasising the issue that, if its use would make sense for some provisions, it is unclear why it would not have made sense for all: NA Smuha, 'The Paramountcy of Data Protection Law in the Age of AI (Acts)', in EDPS (ed), *Two decades of personal data protection. What next? EDPS 20th Anniversary, Luxembourg: Publications Office of the European Union* (2024), p 231.

[25] Recital 38 AI Act. Article 10 LED Article 10 establishes that, under the LED, the processing of special categories of personal data shall be allowed only where strictly necessary, subject to appropriate safeguards for the rights and freedoms of the data subject, only: (a) where authorised by Union or Member State law; (b) to protect the vital interests of the data subject or of another natural person; or (c) where such processing relates to data which are manifestly made public by the data subject.

[26] Additionally, Recital 39 clarifies that any processing of biometric data and other personal data involved in the use of AI systems for biometric identification, other than in connection to the use of real-time remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement as regulated by the AI Act, should continue to comply with all requirements resulting from Article 10 of Directive (EU) 2016/680.

[27] Recital 94 AI Act states that '(a)ny processing of biometric data involved in the use of AI systems for biometric identification for the purpose of law enforcement needs to comply with Article 10 of Directive (EU) 2016/680, that allows such processing only where strictly necessary, subject to appropriate safeguards for the rights and freedoms of the data subject, and where authorised by Union or Member State law'. It is unclear what this Recital might be attempting to clarify; it can in any case be read in the sense that to the extent that the AI Act is not applicable to some processing of biometric data involved in the use of AI systems for biometric identification for the purpose of law enforcement (for instance, because the processing concerns post-remote biometric identification) the LED remains applicable.

cannot rely on the AI Act nor on the grounds listed in Article 10 of the LED to process any data or use any AI system outside of this framework. This seems to close the door to national or EU law authorising additional processing of the biometric data at stake. Furthermore, Recital 38 underlines that the 'AI Act is not intended to provide' a legal basis for the processing of personal data under Article 8 of the LED, meaning the relevant competent authorities shall in any case need to comply with the LED general requirements of lawfulness of processing of personal data.

Finally, Recital 3 of the AI Act goes on to proclaim that, in the light of the recourse to Article 16 of the TFEU, 'it is appropriate to consult the European Data Protection Board' (EDPB). This might presumably refer to the obligation imposed by Regulation (EU) 2018/1725[28] on the European Commission to consult not only the European Data Protection Supervisor (EDPS), but also the EDPB, in the context of legislative procedures that are 'of particular importance for the protection of individuals' rights and freedoms with regard to the processing of personal data'.[29]

34.1.5. The Data Protection *Acquis* as a (Not to be Undermined) Foundation

The EU data protection *acquis* is introduced by the AI Act as the foundation for 'sustainable and responsible data processing',[30] 'including where data sets include a mix of personal and non-personal data'.[31] Recital 10 refers indeed to the GDPR, the EU DPR, the LED Directive and the e-Privacy Directive as such providing such a foundation.

This vision is then directly connected to the assertion that the AI Act 'does not seek to affect the application of existing' EU data protection law,[32] and this idea is subsequently further developed in relation to the actors most notably concerned by EU data protection law. The AI Act, Recital 10 specifies, does not seek to affect the tasks and powers of data protection authorities (DPAs),[33] nor the obligations of providers and deployers of AI systems in their roles as controllers or processors, nor the rights and guarantees awarded to data subjects. On the contrary, it adds, the AI Act should even 'facilitate the effective implementation and enable the exercise of the data subjects' rights and other remedies' guaranteed under EU data protection law 'and of other fundamental rights', a contention for which no further explanation is provided.

As a foundation of the AI Act, the EU data protection *acquis* is not only something that should not be put in jeopardy or hindered, but also something to build upon and further develop. In this sense, it should be kept in mind that, because data protection is a fundamental right, all references in the AI Act to the need to identify and mitigate risks for fundamental rights must

[28] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (Text with EEA relevance.)

[29] *cf* Article 42(2) of Regulation (EU) 2018/1725.

[30] Recital 10 AI Act.

[31] ibid.

[32] ibid.

[33] In this sense, also, Recital 159 AI Act points out, in relation to the access by market surveillance authorities responsible for high-risk AI systems in the area of biometrics used for the purposes of law enforcement, migration, asylum and border control management, or the administration of justice and democratic processes, that these authorities 'should have effective investigative and corrective powers, including at least the power to obtain access to all personal data that are being processed'. After that, the Recital warns that 'any limitations of access to sensitive operational data under the AI Act 'should be without prejudice to the powers conferred' to authorities under the LED, and that '(n)o exclusion on disclosing data to national data protection authorities' under the AI Act should affect the current or future powers of those authorities beyond the scope of the AI Act.

be read as referring also to risks for data protection. This is the case, for instance, of the risk-management system to be run throughout the lifecycle of high-risk AI systems,[34] but also of other requirements such as record-keeping, transparency and the provision of information to deployers, and human oversight.[35] Recital 67 notes that in order to facilitate compliance with EU data protection law, such as the GDPR, the AI Act's 'data governance and management practices should include, in the case of personal data, transparency about the original purpose of the data collection'. Recital 69 stresses that the 'right to privacy and to protection of personal data must be guaranteed throughout the entire lifecycle of the AI system', recalling that 'the principles of data minimisation and data protection by design and by default, as set out in Union data protection law, are applicable when personal data are processed'. In this regard, it puts forward that providers *may* ensure compliance with those principles with measures such as anonymisation and encryption, but also with 'the use of technology that permits algorithms to be brought to the data and allows training of AI systems without the transmission between parties or copying of the raw or structured data themselves'.[36]

This idea that the EU data protection *acquis* is a necessary underpinning of the AI Act, to be respected and reinforced, can be contrasted with subsequent attempts, led by the European Commission, to modify such *acquis*, and to do so notably in the name of supporting AI innovation. There is no call in the AI Act to directly, substantially transform EU data protection law, although a will to move in such direction would become visible in 2025 in the European Commission's work on a Digital Omnibus on Data and a Digital Omnibus on AI – and target very directly the modification of the GDPR, which the AI Act had managed to leave not unchanged, but nevertheless untouched.

34.2. The AI Act and the GDPR

The interplay between the AI Act and the GDPR is marked by the described overall connections between the AI Act and EU data protection law. The fact that the AI Act partly builds on the GDPR is particularly visible in the way it explicitly incorporates some key GDPR definitions: Article 3(50) AI Act establishes that 'personal data' for the AI Act means 'personal data' as defined in Article 4(1) GDPR; Article 3(51) AI Act, that 'non-personal data' for the AI Act means data other than personal data as defined in Article 4(1) GDPR; and Article 3(52) AI Act, that 'profiling' means profiling as defined in Article 4(4) GDPR.

Article 2(7) AI Act states, as noted, that the AI Act does affect the GDPR, or the EU DPR, or the e-Privacy Directive, or the LED, 'without prejudice to Article 10(5) and Article 59 of this Regulation'. This triggers the question of whether and to what extent these two provisions, Article 10(5) and Article 59 AI Act, affect the GDPR and other EU data protection instruments.

This section zooms in on some of the concrete intersections between the AI Act and the GDPR. It does not aim to cover all aspects in which there is or might be some connection, which are numerous (for instance, the notion of 'human oversight' in the AI Act[37] is undoubtedly somehow indebted to the notion of 'human intervention' in Article 22(3) GDPR, on automated individual decision-making), and might actually permeate the totality of the text.

[34] In this sense, Recital 65 AI Act.
[35] In this sense, Recital 66 AI Act.
[36] While further adding 'without prejudice to the requirements on data governance provided for in this Regulation'.
[37] See Recital 73, and Article 14 AI Act.

34.2.1. Processing of Special Categories of Data to Detect and Correct Bias

Article 10(5) AI Act states that '(t)o the extent that it is strictly necessary for the purpose of ensuring bias detection and correction in relation to the high-risk AI systems' as prescribed by the AI Act,[38] the providers of high-risk AI systems 'may exceptionally process special categories of personal data, subject to appropriate safeguards for the fundamental rights and freedoms of natural persons'. The processing of so-called 'special categories of data' (also known as 'sensitive data'), that is, 'personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership', as well as genetic data, biometric data processed for the purpose of uniquely identifying a natural person, and 'data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited' is in principle prohibited under the GDPR, by its Article 9(1). Article 9(2) of the GDPR establishes exceptions in which such general prohibition of processing of sensitive data shall not apply. In line with Article 10(5) AI Act, in addition to the relevant provisions as set out in the GDPR, the EU DPR and the LED, a series of conditions must also be met for this exceptional processing of special categories of data in the name of bias detection and correction to take place.

Concretely, the additional conditions to be respected aim to assert the necessity of the processing ('the bias detection and correction cannot be effectively fulfilled by processing other data, including synthetic or anonymised data'),[39] to provide necessary safeguards ('subject to technical limitations on the re-use of the personal data, and state-of-the-art security and privacy-preserving measures, including pseudonymisation',[40] and 'to measures to ensure that the personal data processed are secured, protected, subject to suitable safeguards, including strict controls and documentation of the access, to avoid misuse and ensure that only authorised persons have access to those personal data with appropriate confidentiality obligations',[41] and ensuring that 'the special categories of personal data are not to be transmitted, transferred or otherwise accessed by other parties'[42]), and to comply with the principles of purpose and storage limitation (the special categories of personal data most be 'deleted once the bias has been corrected or the personal data has reached the end of its retention period, whichever comes first'[43]).

A final additional condition to be complied with adds a specific obligation for records of processing activities under the GDPR, the EU DPR or the LED to include 'the reasons why the processing of special categories of personal data was strictly necessary to detect and correct biases, and why that objective could not be achieved by processing other data'.[44] Nothing is said in the AI Act about whether this obligation is a general obligation, and all controllers and processors must thus include the described reasons in their records of processing activities, or whether the controllers or processors exempted from the general obligations related to keeping records of processing activities would not have to include them. Currently, this omission is not a problem, as Article 30(5) GDPR, which establishes that GDPR record keeping obligations do not apply to enterprises or organisations employing fewer than 250, states nevertheless that the record keeping obligations will always apply when there is processing of special categories of data.

[38] In accordance with Article 10(2)(f) and (g) AI Act.
[39] Article 10(5)(a) AI Act.
[40] Article 10(5)(b) AI Act.
[41] Article 10(5)(c) AI Act.
[42] Article 10(5)(d) AI Act.
[43] Article 10(5)(e) AI Act.
[44] Article 10(5)(f) AI Act.

The interplay between the AI Act and the GDPR in this regard might become slightly more complex if the amendment to Article 30(5) of the GDPR proposed by the European Commission in May 2025 is adopted. In line with that proposal, the GDPR limitation to the exemption for some enterprises and organisations would apply to the cases where 'the processing it carries out is likely to result in a high risk to the rights and freedoms of data subjects, within the meaning of Article 35'[45] GDPR. Article 35(1) GDPR connects the likelihood to result in a high risk to the rights and freedoms of natural persons to the nature, scope, context and purposes of the processing, while Article 35(3)(b) establishes an obligation to carry out a data protection impact assessment if there is processing of special categories of data on a large scale. It might be possible to argue that if special categories of data are processed for ensuring bias detection and correction in relation to the high-risk AI systems, some of these conditions will be met, and thus enterprises and organisations, regardless of their size, cannot be exempted from the specific AI Act obligation established in Article 10(5)(f) AI Act. This conclusion could, however, also be debated in some instances. This uncertainty might surface as a problem in the hypothetical case that such an obligation would not apply when controllers and processors are exempted by the GDPR from their record-keeping obligations, which, it must be stressed, remains unclear.

The question of whether Article 10(5) AI Act affects the GDPR itself is set aside by Recital 70 AI Act, which observes that this processing of special categories of personal data for bias detection and correction in relation to the high-risk AI systems, as allowed by the AI Act, is to take place 'as a matter of substantial public interest within the meaning of Article 9(2), point (g) of Regulation (EU) 2016/679'. Article 9(2)(g) GDPR provides indeed that it is possible to exceptionally process special categories of personal data when such 'processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law'.[46] The AI Act might be interpreted as a law asserting the substantial public interest nature of this processing. In doing so, it opens a door that was left unlocked in the GDPR, allowing for the processing of personal data not allowed before, but it does not change the text of the GDPR. It is important to note that, strictly speaking, and despite the use of the term 'exceptionally', Article 10(5) AI Act does not constitute an 'exception' to the application of the GDPR.[47]

34.2.2. Further Processing in AI Regulatory Sandboxes

Article 59 AI Act is the other provision highlighted in Article 2(7) AI Act as having a particular status, in the sense that the AI Act would not affect the GDPR, 'without prejudice to' some provisions. The subject matter of Article 59 AI Act is the 'further processing of personal data for developing certain AI systems in the public interest in the AI regulatory sandbox'. The Article establishes that, in an AI regulatory sandbox, personal data lawfully collected for other

[45] In full, the proposed provision reads: 'The obligations referred to in paragraphs 1 and 2 shall not apply to an enterprise or an organisation employing fewer than 750 persons unless the processing it carries out is likely to result in a high risk to the rights and freedoms of data subjects, within the meaning of Article 35' (European Commission, Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2016/679, (EU) 2016/1036, (EU) 2016/1037, (EU) 2017/1129, (EU) 2023/1542 and (EU) 2024/573 as regards the extension of certain mitigating measures available for small and medium sized enterprises to small mid-cap enterprises and further simplification measures, COM(2025) 501 final, Brussels, 21.5.2025, p 6).

[46] Law 'which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject' (Article 9(2)(g) GDPR).

[47] Using the term 'exception', for instance: M van Bekkum, 'Using Sensitive Data to De-bias AI Systems: Article 10(5) of the EU AI Act' [2025] 56 *Computer Law & Security Review* 106115.

purposes may be processed, but solely for the purpose of developing, training and testing certain AI systems and when certain conditions are met[48] (conditions that include, for instance, that the data processed must be necessary for complying with at least a requirement referred to in Chapter III, Section 2 of the AI Act and it is not possible to effectively fulfil such requirement by processing anonymised, synthetic or other non-personal data).[49] As the personal data at stake were originally collected for other purposes, different from the developing, training and testing pursued, the processing hereby allowed is described as 'further processing'.

According to Recital 140 AI Act, the AI Act 'should provide the legal basis for the providers and prospective providers in the AI regulatory sandbox to use personal data collected for other purposes for developing certain AI systems in the public interest within the AI regulatory sandbox, only under specified conditions, in accordance with' Articles 6(4) and 9(2)(g) GDPR.[50] This is indeed the function of Article 49 AI Act: to provide such a 'legal basis', or what is described as such in the words of the AI Act, even though it is debatable that, from a GDPR perspective, that was the best terminological choice.

Article 59 AI Act builds thus primarily on Article 6(4) GDPR, that is, the last paragraph of Article 6 GDPR, on 'Lawfulness of processing'. This last paragraph describes how the controller can ascertain whether some data processing for a purpose other than the purpose for which data had originally been collected is to be deemed 'compatible', and allow for such further processing to take place despite the purpose limitation principle, which establishes that personal data cannot be 'further processed in a manner that is incompatible with' the purposes for which it was collected.[51] According to Recital 50 GDPR, when this kind of 'further processing' takes place, 'no legal basis separate from that which allowed the collection of the personal data is required'. Therefore, Article 6(4) GDPR does not, strictly speaking, constitute or refer to any legal basis for processing, but rather describes criteria that help determine the situations in which an additional legal basis is not required. Regarding Article 9(2)(g) GDPR, it allows for the further processing of special categories of data when such processing is necessary for reasons of substantial public interest.

34.2.3. Biometric Data

The definition of biometric data in the AI Act does not correspond to the definition of biometric in the EU personal data protection *aquis*. This was not supposed to happen: the original proposal of the European Commission simply imported the definition of biometric data from the GDPR. During the legislative process, however, discussions surfaced[52] about the scope of terms dependent on the notion of biometric data, which was eventually expanded.

Article 4(14) GDPR defines 'biometric data' as (14) 'personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of

[48] Article 59(1) AI Act.

[49] Article 59(1)(b) AI Act.

[50] Also in accordance with Articles 5, 6 and 10 of Regulation (EU) 2018/1725, and without prejudice to Article 4(2) and Article 10 of Directive (EU) 2016/680. Recital 140 AI Act observes that all other obligations of data controllers and rights of data subjects under Regulations (EU) 2016/679 and (EU) 2018/1725 and Directive (EU) 2016/680 remain applicable. In particular, this Regulation should not provide a legal basis in the meaning of Article 22(2) GDPR.

[51] Article 5(1)(b) GDPR.

[52] See, in this sense: G González Fuster and M Nadolna Peeters (2021), *Person identification, human rights and ethical principles: Rethinking biometrics in the era of artificial intelligence*, Panel for the Future of Science and Technology, European Parliamentary Research Service (EPRS), Scientific Foresight Unit (STOA) PE 697.191 – December 2021.

a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data'. In the AI Act, biometric data are defined (in its Article 3(34)) in exactly the same terms, except for the words 'which allow or confirm the unique identification of that natural person'. This is an extremely significant difference, as the deleted reference to the possibility of uniquely identifying someone is crucial, in the context of the GDPR, to determine the special nature of biometric data. In this sense, Article 9(1) of the GDPR brings to the fore again such potential for unique identification, establishing that the processing of 'biometric data for the purpose of uniquely identifying a natural person' shall constitute processing of 'special categories of personal data' and as such be in principle prohibited. Recital 51 GDPR explicitly connects the possibility for unique identification or authentication of a natural person to the particular sensitivity of some data, the processing of which can create significant risks to the fundamental rights and freedoms, which justify their 'special' treatment.

The AI Act definition of biometric data is on paper broader than the GDPR definition, as it is not limited to data allowing or confirming the unique identification of persons. In this sense, Recital 14 AI Act points out that biometric data can allow not only for identification but also for the categorisation of natural persons, as well as 'for the recognition of emotions of natural persons'. Recital 14, however, also argues that the AI Act notion of 'biometric data' 'should be interpreted in light of the notion of biometric data as defined in' Article 4(14) GDPR, Article 3(18) EU DPR and Article 3(13) LED. This statement is, to say the least, enigmatic, knowing as we know that the AI Act definition is different, and that it is different because of a deliberate choice of the legislator. As both are manifestly different, it is unclear what the presumed implications of reading the former 'in light of' the latter are, an exercise akin to interpreting an apple in light of a pear, or the day in light of the night.

Whereas the definition of biometric data differs in the AI Act and in the GDPR, the notion of 'special categories of personal data', which includes a reference to biometric data, is presented in both instruments as being the same.[53] Article 3(37) AI Act states indeed that the notion of 'special categories of personal data' concerns the categories of personal data referred to in Article 9(1) GDPR.[54] This could seem paradoxical because it implies that two totalities are identical despite one of their shared elements being openly not identical between them. A possible way to attenuate the conceptual tensions in this paradox is to remember that Article 9(1) GDPR explicitly refers to the need to process biometric data 'for the purpose of uniquely identifying a natural person' for such processing to be regarded as processing of special categories of data, a reference that in a way compensates the omission of this requirement in the very definition of biometric data in the AI Act. The relationship between these notions appears however again conceptually complicated when Recital 54 AI Act interjects that 'biometric data constitutes a special category of personal data' referring to the AI Act. This would appear to mean that the broader AI Act notion of biometric data (not requiring to 'allow or confirm the unique identification of that natural person') is part of the AI Act notion of 'special categories of data', making it very difficult to pretend that this notion is still identical, or even equivalent to, the GDPR notion of special categories of data.

The AI Act notion of biometric data is, in any case, extremely important for the whole AI Act architecture, as it notably determines the scope of the notion of biometric categorisation

[53] Strictly speaking, there is no 'definition' of special categories of data in the GDPR.
[54] And similarly in Article 10 LED and in Article 10(1) EU DPR.

systems[55] and of emotion recognition systems.[56] It is also very relevant for the regulation of real-time remote identification.

As mentioned above, the prohibition of the use of AI systems for real-time remote biometric identification of natural persons in publicly accessible spaces for the purpose of law enforcement, and their possible use subject to certain exceptions, apply as *lex specialis* in respect to Article 10 of Directive (EU) 2016/680', according to a Recital.[57] Article 5(1)(h) AI Act clarifies, presumably to avoid some potential ambiguity, that such prohibition and the related possible exceptions apply 'without prejudice to Article 9' of the GDPR for the processing of biometric data for purposes other than law enforcement. In a similar vein, Recital 39 states that '(f)or purposes other than law enforcement, Article 9(1) of Regulation (EU) 2016/679 and Article 10(1) of Regulation (EU) 2018/1725 prohibit the processing of biometric data subject to limited exceptions as provided in those Articles' – which appears somehow elliptically to refer to the processing for real-time remote biometric identification in publicly accessible spaces for purposes other than law enforcement. Recital 39 concludes noting that under Article 9(1) of the GDPR, 'the use of remote biometric identification for purposes other than law enforcement has already been subject to prohibition decisions by national data protection authorities'. This could be read in the sense that, because such processing has sometimes been prohibited, there was no need for the AI Act to prohibit it, or as a mere reminder.

34.2.4. Fundamental Rights Impact Assessment Obligations

By virtue of Article 27 AI Act, some deployers of high-risk AI systems (mainly, bodies governed by public law, and private entities providing public services) shall perform a fundamental rights impact assessment before the deployment. The same Article provides, however, that if any of the AI Act obligations related to fundamental rights impact assessments 'is already met through the data protection impact assessment conducted pursuant to Article 35' of the GDPR (or Article 27 LED), the fundamental rights impact assessment 'shall complement that data protection impact assessment'.[58]

Strictly speaking, the provision does not state that if an obligation is already met by conducting a GDPR data protection impact assessment, there would be no need to comply with the equivalent AI Act obligations related to fundamental rights impact assessment. It rather seems to imply that in such a case, the GDPR impact assessment takes a sort of prominent role, and that it is to be complemented by the FRIA.

34.2.5. Information to be Submitted by Deployers

Annex VIII of the AI Act specifies the information to be submitted upon the registration of high-risk AI systems in accordance with Article 49 AI Act. Section C of this Annex lists more concretely the information to be submitted, before putting into service or using a high-risk

[55] See Article 3(40) AI Act: biometric categorisation system 'means an AI system for the purpose of assigning natural persons to specific categories on the basis of their biometric data, unless it is ancillary to another commercial service and strictly necessary for objective technical reasons'; also Recital 16 AI Act.

[56] See Article 3(39) AI Act: emotion recognition system 'means an AI system for the purpose of identifying or inferring emotions or intentions of natural persons on the basis of their biometric data'.

[57] Recital 38 AI Act.

[58] Article 7(4) AI Act.

AI system listed in Annex III AI Act,[59] by deployers of high-risk AI systems that are public authorities, EU institutions, bodies, offices or agencies or persons acting on their behalf, in accordance with Article 49(3) AI Act.

The information to be provided and thereafter kept up to date with regard to high-risk AI systems registered in accordance with Article 49(3) includes both a summary of the findings of the fundamental rights impact assessment conducted in accordance with Article 27 AI Act,[60] and a summary of the data protection impact assessment carried out in accordance with Article 35 GDPR (or Article 27 LED) 'as specified in Article 26(8) of this Regulation, where applicable'. The reference to Article 26(8) AI Act is manifestly a typo, and should be read as a reference to Article 26(9) AI Act, which states that 'where applicable, deployers of high-risk AI systems shall use the information provided under Article 13 of this Regulation to comply with their obligation to carry out a data protection impact assessment under Article 35' GDPR or Article 27 LED.

The information referred to in Article 26(9) AI Act concerns the instructions that must accompany high-risk AI systems,[61] and more generally, the imperative 'appropriate type and degree of transparency' to be ensured with a view to achieving compliance with the relevant obligations of the providers and deployers.[62] This can be perceived as a multiplication of recording obligations and modulations of such obligations which somehow end up imposing formal work of very unclear added value: in some cases, deployers of high-risk AI systems are thus supposed to be able to re-use some information already provided (under Article 13 AI Act) in order to comply with their data protection impact assessment GDPR obligations, and then they will be asked to provide a summary of the same information they have been copying and pasting – and to which they could have perhaps just referred to.

34.2.6. Consent to Real-World Testing

Under the AI Act, providers and prospective providers of high-risk AI systems can test them in real-world conditions without participating in an AI regulatory sandbox.[63] To protect the individuals participating in such real-world testing, the AI Act bets on requesting from them 'informed consent' to participate.[64]

Recital 141 AI Act affirms that the consent of subjects to participate in real-world testing 'is distinct from, and without prejudice to, consent of data subjects for the processing of their personal data under the relevant data protection law'. This clarification is convenient to avoid any possible confusion, for instance, in relation to the need to inform participants about the possibilities regarding any possible requesting of the reversal or the disregarding of the predictions, recommendations or decisions of the AI system,[65] which is presumably to involve personal data

[59] With the exception of high-risk AI systems listed in point 2 of Annex III.
[60] Annex VIII, Section C, point 4.
[61] Article 13(2) and 13(3) AI Act.
[62] Article 13(1) AI Act.
[63] Article 60 AI Act. The AI Act also regulates the transfer of data – both personal and non-personal data – collected and processed for the purpose of testing in real-world conditions. As Recital 141 AI Act notes, data 'should be transferred to third countries only where appropriate and applicable safeguards under Union law are implemented, in particular in accordance with bases for transfer of personal data under Union law on data protection, while for non-personal data appropriate safeguards are put in place in accordance with Union law, such as Regulations (EU) 2022/868 (42) and (EU) 2023/2854 (43) of the European Parliament and of the Council'.
[64] With the exemption of testing for law enforcement (Recital 141 AI Act).
[65] Article 61(1)(d) AI Act.

processing. In this sense, Recital 141 AI Act notes that 'it is appropriate to envisage additional safeguards to ensure that the predictions, recommendations or decisions of the AI system can be effectively reversed and disregarded and that personal data is protected and is deleted when the subjects have withdrawn their consent to participate in the testing without prejudice to their rights as data subjects under the Union data protection law'.

34.2.7. Some Less Fortunate References

Some additional explicit and implicit references to the GDPR in the AI Act have to be highlighted because they might be regarded as of particularly limited value in terms of legal certainty. In this sense, for instance, whereas Article 86 of the AI Act establishes a 'right to an explanation', the same Article also states that such right to an explanation 'should apply only to the extent this right is not already provided for under Union law'.[66] This triggers the question of the extent to which the same right is provided or not under the GDPR.[67]

By virtue of Article 47 AI Act, providers have to draw up an EU declaration of conformity for each high-risk AI system. Such declaration must include a statement stating that the AI system is in conformity with the AI Act,[68] and, when the AI system 'involves the processing of personal data, a statement that that AI system complies with Regulations (EU) 2016/679 and (EU) 2018/1725 and Directive (EU) 2016/680'. The wording of this sentence is unfortunate, as it is legally impossible for a processing operation to comply with the GDPR *and* the EU DPR *and* the LED.

Finally, Article 50(3) AI Act establishes that 'deployers of an emotion recognition system or a biometric categorisation system shall inform the natural persons exposed thereto of the operation of the system, and shall process the personal data in accordance with Regulations (EU) 2016/679 and (EU) 2018/1725 and Directive (EU) 2016/680, as applicable'. This reference to the imperative of complying with EU data protection law was technically unnecessary, as it is in principle undisputable that they have to process personal data in accordance with the law. The mention could have been welcomed as a general reminder had it not been followed by an ambiguous sentence, which brings more trouble than clarity, and starts with these words: 'This obligation shall not apply to AI systems used for biometric categorisation and emotion recognition, which are permitted by law to detect, prevent or investigate criminal offences'.[69] It is unclear to what exactly the term 'this obligation' refers in the second sentence of Article 50(3). Presumably, the message the sentence is trying to convey is that deployers are not obliged to inform in certain cases. The sentence construction, however, seems to hint that it could be the obligation to process personal data complying with the law that does not apply in certain cases.

34.3. Final Remarks

Data protection matters for the AI Act. And the AI Act matters for data protection. The AI Act builds upon the GDPR modulating its legal impact, but without directly contradicting it

[66] Recital 171.
[67] See Ch 30 in this Commentary.
[68] Point 4 of Annex V AI Act.
[69] Only if 'subject to appropriate safeguards for the rights and freedoms of third parties, and in accordance with Union law' (Article 50(3) AI Act).

or affecting its scope of application, avoiding major damage. In doing so, it illustrates that it is possible to legislate to support the deployment of AI while respecting EU fundamental rights protection, certainly on paper and at least to some extent. Although it is certainly arguable that the elements of the AI Act directly based on Article 16 TFEU might actually have seriously brought down the level of personal data protection in the EU (by granting law enforcement new, significant powers to use AI), as far as the GDPR is concerned, the negative effects of the adoption of the AI Act are relatively limited.

Historically, there is a continuity between the thinking that led to the development of EU data protection law and more recent concerns that surround modern AI regulation. It is possible to highlight that such continuity made data protection the best-suited body of law to regulate AI.[70] It could have been hoped that such continuity would prevent the regulation of AI from becoming bad news for data protection.

Eventually, however, the adoption of the AI Act might nevertheless turn out to have an indirect negative effect on the GDPR. If the AI Act was supposed to be a step forward in the path towards reinforced fundamental rights protection, it seems now to be hitting back at the GDPR like a boomerang. It is certainly being used for such purposes by a variety of actors,[71] who are stressing some of the tensions between the AI Act and the GDPR to call not only for a simplification or clarification of their interplay, but actually for further legislative changes in the AI Act and in the GDPR.

Politically speaking, the AI Act certainly did not manage to achieve closure in terms of soothing all anxieties generated by the processing of personal data for AI purposes, be it, for instance, in relation to the need for a legal basis for AI training,[72] or on the question of how to comply with data subject rights. On top of that, it brought extra concerns about possible unnecessary overlaps, or about what some liked to describe as inconsistencies, or a cry for synergies.[73]

Despite some initial efforts by some data protection authorities to appease some major tensions,[74] and the promises of the EDPB to develop guidelines before the end of 2027,[75] the pressure towards future legislative carnage might be stronger. It seems that in the perpetual battle for preserving and promoting the EU's fundamental rights, the AI Act was perhaps too easily weaponised and led in the wrong direction.

[70] G Zanfir-Fortuna, 'Why Data Protection Legislation Offers a Powerful Tool for Regulating AI – EUROPP' (*EUROPP – European Politics and Policy*, 10 February 2025) https://blogs.lse.ac.uk/europpblog/2025/02/10/why-data-protection-legislation-offers-a-powerful-tool-for-regulating-ai/ accessed 1 September 2025.

[71] See, for instance, referring to rules duplication, uncertainty, ambiguity and inconsistencies: H Graux et al, *Interplay between the AI Act and the EU digital legislative framework*, Policy Department for Transformation, Innovation and Health Directorate-General for Economy, Transformation and Industry, European Parliament, PE 778.575, October 2025.

[72] See, in this sense, for instance: EDBP, *Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models*, adopted on 17 December 2024.

[73] In the spring of 2025, the Polish Presidency of the Council of the EU proposed a joint discussion between members of the Working Party on Data Protection (WP DATAPROTECT) and of the Working Party on Telecommunications and Information Society (WP TELECOM), with the explicit purpose of exploring 'best practices to ensure synergies in the application of the GDPR and the AI Act' (Presidency of the Council of the EU, 'Joint Discussion on the Application of the GDPR and the AI Act – Discussion Paper' 2).

[74] The data protection authority of Luxembourg, for instance, posted in February 2025 a short text noting that many of the AI systems prohibited by the AI Act would in any case involved personal data processing that would be problematic: 'Les systèmes d'IA prohibés selon l'AI Act : impact sur la protection des données personnelles' (7 February 2025) http://cnpd.public.lu/fr/dossiers-thematiques/intelligence-artificielle/regulation-ia/ia-prohibes.html accessed 1 September 2025.

[75] See the EDPB's 'Strategy 2024–2027': 'We will provide guidance on the interplay between the application of the GDPR and other EU legal acts, particularly the EU Artificial Intelligence Act' (April 2024, www.edpb.europa.eu/our-work-tools/our-documents/strategy-work-programme/edpb-strategy-2024-2027_en).