Comments about the EDPB draft Guidelines 02/2025 on processing of personal data through blockchain technologies

This paper exclusively reflects the views of its author.

On 14 April 2025, the European Data Protection Board published its draft Guidelines 02/2025[1] *"on processing of personal data through blockchain technologies"* (hereinafter referred to as Draft Guidelines or Draft).

These comments below would like to raise the awareness of a higher-level issue, namely the unsuitability of GDPR for regulating all kinds of activity where personal data are involved.

1. The material scope of the GDPR – based on the example of blockchain

When I speak of 'processing' in this chapter, I am not referring to the concept of 'processing' within the meaning of Article 4(2) of the GDPR,[2] but to the concept of 'processing' within the meaning of Article 2(1) of the GDPR, which defines the material scope of the GDPR, and which is not specifically defined in the GDPR, but merely denoted by adjectives.

The difference between Article 2(1) and Article 4(2) of the GDPR must be emphasised because if an activity does not fall within the material scope of the relevant legislation (Article 2), what is included in the definition of processing (Article 4) is completely irrelevant.[3]

The French Data Protection Authority (CNIL), in its position paper on the data protection issues of blockchain (more precisely, its compliance with the GDPR), states that the GDPR and, more broadly, the classic data protection principles were developed in a world in which the processing of data was *centralised* within the organisation of specific entities (controllers). In this regard, the *decentralised data processing model* used by blockchain technology and the multitude of actors involved in data processing lead to a more complex definition of their roles.[4] The CNIL therefore describes the system of data processing described/regulated in the GDPR as a centralised data processing model, whereas the system of blockchain is described as a *decentralised* model, which is different from the centralised model.

[1] https://www.edpb.europa.eu/system/files/2025-04/edpb_guidelines_202502_blockchain_en.pdf

[2] ''Processing'': *any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction'.*

[3] While the 'household exception' may involve collection, recording, organisation, storage, adaptation or alteration, erasure or destruction, they should not be judged in accordance with the GDPR.

[4] *"„The GDPR, and more broadly classical data protection principles, were designed in a world in which data management is centralised within specific entities. In this respect, the decentralised data governance model used by blockchain technology, and the multitude of actors involved in the processing of data lead to a more complex definition of their role."* Cf. CNIL (2018): Solutions for a responsible use of the blockchain in the context of personal data. Downloaded: https://www.cnil.fr/sites/default/files/atoms/files/blockchain_en.pdf (Last download: 9 June 2022.)

The CNIL does not appear to have realised that, by the two sentences quoted, it is actually referring to the material scope of the GDPR, namely Article 2(1) of the GDPR. The CNIL is right that the classic data protection principles in the broad sense were formulated at a time when 'processing' meant centralised, isolated, automated databases, in relation to which the number of actors involved in the processing was very limited and their roles clearly distinguishable.[5] A body of legislation imprinting 'classical data protection principles' (Council of Europe Convention 108 or Directive) regulated this technical environment, such 'processing activities', and what is more important: it was suitable for this purpose. [6] The GDPR has not made any substantive changes in this regard.

The fault of data protection practice (and regulation) is that the legislator and (most of) the data protection practitioners have considered that 'processing activity' forms a homogeneous block and that the same rules apply to all types of processing.[7] The picture in the GDPR is more nuanced that both the large number of empowerments for Member States[8] and Chapter IX of the GDPR[9] indicate that there are areas where the legislator also thought that a different approach might be justified. On the substance, however, this does not change the concept of the GDPR as a 'centralised model'. Furthermore, if we look at some of the new institutions of the GDPR (e.g. data portability or profiling), they are also more connected to database-based data processing than to data processing under other models.

By contrast, blockchain has challenged a number of GDPR rules and GDPR-compliant solutions can be found only with 'strong trade-offs', which, however, challenge the essence of the technology.[10] It should be noted, however, that even before blockchain, there were data processing operations that could not or could hardly be included in the rules embodying the

[5] See Resolutions of the Committee of Ministers of the Council of Europe of 1973 and 1974 specifically on "electronic databases" [Resolution (73) 22 on the protection of the privacy of individuals vis-a-vis electronic data banks in the private sector. Downloaded: https://rm.coe.int/1680502830 and Resolution (74) 29 on the protection of the privacy of Individuals vis-a-vis electronic data banks in the public sector. Downloaded: https://rm.coe.int/16804d1c51 Last download: 9 June 2022]. A similar assessment is made by Marija Boskovic Batarelo LL.M.: Blockchain and GDPR – friends or foes? Downloaded: https://parser.hr/en/blockchain-and-gdpr-friends-or-foes/ (Last download: of 9 June 2022)

[6] Convention 108 of the Council of Europe is also essentially about the protection *of individuals with regard to automatic processing of personal data,* and it is only optional to extend it to manual processing. Directive 95/46/EC also gave Member States 12(!) years to bring their rules on the processing of data stored in the manual filing system into line with the Directive (cf. Article 32(2) of the Directive), i.e. it cannot in the least be said that the Directive regulated both types of data processing, but the priority is clearly visible: regulating 'automated' data processing.

[7] The fact that neither Council of Europe Convention 108 nor the Directive laid down specific rules for manual data processing, but also considered the rules on computer processing to be applicable to them, has formally established the 'technological neutrality' of data protection rules, but it would be difficult to say that it has actually been implemented.

[8] In particular, an almost unlimited authorisation for derogation regarding the processing of health data.

[9] Provisions relating to specific processing situations

[10] See also. *„[T]he very technical specificities and governance design of blockchain use cases can be hard to reconcile with the GDPR."* - European Parliamentary Research Service (2019): Blockchain and the General Data Protection Regulation. Can distributed ledgers be squared with European data protection law? Downloaded: https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf (Last download: 9 June 2022).

'classic data protection principles'. Suffice it to think of image recording and surveillance systems, but other examples include data processed in any procedure (typically in documents or in other non-pre-structured forms, e.g. audio recordings).

Thus, the assertion that blockchain represents the decentralized model also raises the question of whether blockchain can be included in the scope of the GDPR at all. Can data processing that radically deviates from the model regulated in the GDPR fall within the scope of the GDPR, without the law (GDPR) explicitly stating this? Under the Directive 95/46/EC there was no substantive obstacle to such an option (since the applicable rule was created by the Member States), but the GDPR lacks *the mechanisms that would allow for the development of adequate rules,* since legislation can only be amended by legislation: neither the EDPB nor the courts' interpretation of the law should go so far as to change the rules of the GDPR or to (arbitrarily) exclude the application of certain provisions in order to prevent the rule in question from imposing the impossible. Article 23 of the GDPR is in no way capable of invoking it as a basis for derogating from the GDPR in relation to new technologies.

2. Complexity of the range of actors involved in the application of new technologies

In the era of 'classical data protection principles', processing activity was typically the activity of a controller, who also typically involved no more than one processor. Accordingly, the GDPR model also assumes that the range of actors is limited, the roles are clearly defined and the processing activities take place in one (or only a few) place.[11] This can only be said exceptionally for new technologies.

One major problem with new technologies is precisely the number of actors involved and the resulting complex systems[12] (either in the area of blockchain, the Internet of Things or cloud computing), including the lack of clarity on data controller/processor roles[13] or the predominant role of the technology provider (e.g. cloud computing or artificial intelligence). For example, cloud service providers consider themselves to be processors[14] (as stated by the

[11] See also. Marija Boskovic Batarelo LL.M.: Blockchain and GDPR – friends or foes? Downloaded: https://parser.hr/en/blockchain-and-gdpr-friends-or-foes/ (Last download: 9 June 2022);

[12] See e.g. Arora, Sandeep (2018): GDPR and challenges driven by the emerging technologies. Downloaded: https://www.linkedin.com/pulse/gdpr-challenges-driven-emerging-technologies-sandeep-arora/ (Last download: 9 June 2022).

[13] See e.g. CNIL (2018), which, as regards the role of miners in relation to blockchain technology, leaves unclear whether they qualify as processors in some cases, contrary to the position of the National Authority for Data Protection and Freedom of Information, which in turn qualifies all actors as controllers. See the position of the National Authority for Data Protection and Freedom of Information on the data protection context of blockchain technology (2017). Downloaded: https://naih.hu/files/Adatved_allasszabas_naih-2017-3495-2-V.pdf (Last download: of 9 June 2022

[14] IBM Cloud Managed Services DPA Exhibit. Downloaded: https://www.ibm.com/support/customer/csol/terms?id=DPA-Exhibit_SMA&lc=en#detail-document (Last download: 9 June 2022) or Google Cloud Data Processing and Security Terms. Downloaded: https://cloud.google.com/terms/data-processing-terms (Last download: of 9 June 2022)

EDPB),[15] but due to the complexity of the technology and service (e.g. the sharing of data between data centres, changes in the data centres, and e.g. the determination of the degree of redundancy), cloud service providers no longer act only 'on behalf of the controller', but are themselves active (if not exclusive) actors in the definition of 'device'. Instead of requiring that complex relationships be 'written down', the law could take on the role of regulating the liability of each actor.

3. Unachievability of the 'classical data protection principles'

New technologies pose a major challenge to all 'classic data protection principles'.[16] Such answers to all these problems should be found that do not hamper the intended functionality of new technologies. This does not mean that new technologies are *ab ovo* good, useful, or that they are *ab ovo* violating the law (violating, for example, human dignity or privacy). Since the *processing* of personal data is necessarily part of a process (ancillary activity), the 'good' nature of new technologies should not be approached solely from the point of view of data processing rules. Sectoral rules should solve this dilemma.

Zsolt Bártfai

[15] See EDPB Guidelines 07/2020 on the concepts of controller and processor under the GDPR, paragraphs 30 and 84. Downloaded: https://edpb.europa.eu/system/files/2021-07/eppb_guidelines_202007_controllerprocessor_final_en.pdf (Last download: of 9 June 2022

[16] El-Gazzar, Rania - Stendal, Karen (2020): Examining How GDPR Challenges Emerging Technologies, In: Journal of Information Policy, 2020, Vol. 10 (2020), p. 237-275. Downloaded: https://www.jstor.org/stable/10.5325/jinfopoli.10.2020.0237 (Last download: of 9 June 2022)