STUDIO LEGALE
GANGI

EDPB
Via electronic form

Paolo Maria Gangi LL.M.
Email pmg@studiogangi.com
Your reference

Date
June 9, 2025

Re feedback in relation to the document "Guidelines 02/2025 on processing of personal data through blockchain technologies".

Dear Sir or Madam,

Following the publication of the document "Guidelines 02/2025 on processing of personal data through blockchain technologies" ("GL") by the EDPB with the possibilities from stakeholders to present comments, by June 9, 2025, this Law Firm would like to make the following observations.

1) The principle of necessity

The entire GL seems to have been written on the basis of a misplaced application of the principle of necessity within the blockchain context. The principle of necessity is enshrined in various GDPR provisions (e.g. Art. 25, par. 2, Art. 35, par.7, b, etc.) and it substantially means that personal data can be processed as far as that process is necessary. In other words, the controller must consistently weigh the need to process personal data against the potential risks associated with that processing. This principle must be applied within the context of each specific situation, considering the specifics rather than making abstract assessments.

A recurring theme in the GL suggests that blockchain is merely a technology and that its implementation might conflict with certain provisions of the GDPR. Therefore, under this idea, it may be advisable for data controllers to consider alternative technical solutions that impose fewer GDPR obligations.. For example: Recommendation 1 (108) states that "*If so, why is a blockchain a necessary and proportionate means for this processing? (i.e. What is the rationale for this choice? What were the eventual alternatives?)*"; par. 7 that "*Blockchains show a number of properties, that create specific non-compliance risks and risks for the rights and freedoms of natural persons when dealing with personal data. For example, once a transaction is recorded on the chain, it cannot individually be*

altered or removed without being detected as an inconsistency in the chain"[1]; par. 47 that "*the choice of this technology among others has to comply with the necessity principle enshrined in GDPR15. It is thus important to document why this has been chosen*".

The reasoning presented above mischaracterizes or fails to acknowledge that today, blockchain technology, especially within major public permissionless networks such as Ethereum, Solana, and Sui, serves not just as a technological framework but has become the chosen system for large communities and social groups to connect and engage with one another. Entire ecosystems of businesses, no-profit entities, activities and groups have daily interaction within the blockchain. It is useless to list here the numbers and the statistics of the communities of the public permissionless blockchains but, as everyone can easily find on Google, they are really huge. The reasons for having adopted the blokchain as a technology are indicated in the same GL where in various paragraphs it is said that the blockchain technology offers a valid framework to implement a disintermediate system among participants[2].

Disintermediation is not just a technical capability; it embodies social and cultural values that empower participants in the crypto ecosystem to build decentralized organizations and engage within a governance structure that traditional centralized databases do not facilitate. Regardless of one's opinion on this phenomenon, it is clear that blockchain technology has become foundational for a vast social group of individuals who interact and operate in public permissionless blockchains. Therefore, the choice it is not only to use or not use the blockchain as a technology but also, and naturally more important, whether or not to be able to be part, for example, to the Ethereum or the Solana or the Sui community. Is it possible to create a DAPP or a system which is aimed at the Ethereum community without making use of the blockchain? Certainly not. Is it possible for a member of the Ethereum community to continue to be a participant in that community without interacting with the blockhain? Certainly not.

If the social and cultural dimension of the blockchain does not solve in itself some tensions that it has as technology with the GDPR the balance of risk under the principle of necessity should be assessed on a very different scale: it should not be risks under GDPR v. one among many, equal, technologies but, rather, risks under GDPR v. exclusion from a social and cultural group such as the Ethereum community or those of the other permissionless public blockchains.

From the perspective of a company aiming to engage with the community of a public,

[1] Footnote 3 at paragraph 3 on pag 3, seems even to have voluntarily adopted an open-biased tone *"e.g. a paradox: While the intention behind using blockchain is often to give users more control over their data, users may end up losing control over their data, owing to the permanent availability of data stored on the blockchain".*

[2] E.g. par. 65: "*A core essence of a blockchain is disintermediation, which is achieved by broadcasting every internal transaction and allowing many-to-many cross checks*".

permissionless blockchain, forgoing blockchain technology essentially equates to forgoing the ability to operate their business. Similarly, for a group seeking to establish themselves as a decentralized autonomous organization (DAO) within the Ethereum ecosystem, not utilizing the blockchain would hinder their ability to create the organizational framework they desire. Even more critically, it would prevent them from connecting with a larger community.

Note 15 at page 11 of the GL cite an excerpt from a case law of the European Court of Human Rights[3]: *"the Court has noted that, whilst the adjective "necessary", within the meaning of Article 10 (2) (art. 10-2), is not synonymous with "indispensable", neither has it the flexibility of such expressions as "admissible", "ordinary", "useful", "reasonable" or "desirable" and that it implies the existence of a "pressing social need*". The desire or the decision by many individuals to join the social groups of the public permissionless blockchains, for all reason stated above, correspond exactly to the notion of a "pressing social need".

2) The role of controller

Section 3.3 of the GL assert that in determining the roles of controllers and processors a factual assessment should be executed while the GL refers substantially to the EDPB guidelines on the concepts of controller and processor in the GDPR, V2.0, adopted on 7 July 2021.

The identification of the controller's role is crucial, particularly regarding GDPR compliance, especially in the context of blockchain technology. This is essential for achieving the balance discussed in the previous section between the principle of necessity and the decision to implement blockchain solutions.

The mere reference to a factual assessment seems not adequate given the academic debate that there has been in relation to what constitutes a controller within a blockchain context. Where some consider nodes to be joint-controllers and other proposed that miners be controllers, within that debate it stands out the position of the French CNIL which write that "*participants, who have the right to write on the chain and who decide to send data for validation by the miners, can be considered as data controllers […] more specifically, the CNIL considers that the participant is a data controller: •when the said participant is a natural person and that the personal data processing operation is related to a professional or commercial activity (i.e. when the activity is not strictly personal); •when the said participant is a legal person and that it registers personal data in a blockchain*"[4].

The CNIL in that report makes the following example: "*if a notary records his or her client's property deed on a blockchain, the said notary is a data controller. In addition, if a bank enters its clients' data onto*

[3] Court (Plenary) - Judgment (Merits) (6538/74) - case of the Sunday Times v. the United Kingdom: 86.96.
[4] *Solutions for a responsible use of the blockchain in the context of personal data*, September 2018, pag. 1.

a blockchain as part of its client management processing, it is a data controller". In other words, DAPPs should be considered controllers in blockchain contexts. This not only makes sense but also brings legal certainty in relation to the process of data within blockchains. We would suggest that the GL go beyond a mere reference to a factual assessment and gives clear indications to which subject should be considered, generally speaking, a controller within blockchain contexts. A reference to the authoritative opinion of the French CNIL could provide legal clarity to operators in this subject matter.

The adoption of the CNIL opinion would also determine the revision of what is indicated in paragraphs 43 and 44 of the GL which state that, in certain circumstances, nodes in public permissionless blockchains can be controllers. If this can be true in some extreme cases, like that of a fork, in general, nodes are not those "which, alone or jointly with others, determines the purposes and means of the processing of personal data"[5]. A clear statement that in most cases DAPPs are controllers would avoid mischaracterizing nodes as controllers.

3) The notion of personal data

The GL asserts that "*metadata of transactions includes both identifiers of the users who are participants of the transactions and other metadata […] If the user is a natural person and those public keys can be used to identify the individuals by means reasonably likely to be used, for example in case of a data breach, then those identifiers qualify as personal data*"[6]. Morever, that "*the EDPB recalls that encrypted personal data is still personal data and encryption does not remove the need for GDPR compliance*"[7] and, finally, that "*it is important to recall that, the GDPR will still apply to that processing activity and that the hash will also be considered personal data, as will any other identifiers that might exist*"[8].

By asserting that metadata, encrypted data, and hashed data qualify as personal data under the GDPR, the EDPB significantly expands the scope of the regulation in the context of blockchains while simultaneously contradicting established case law from the CJEU.

As it is well known, the concept of personal data can be understood through two perspectives. The first, an objective criterion, defines "personal data" under the GDPR as any information that can be used by any third party worldwide to identify a natural person, regardless of whether the entity processing the data has the capability to make that identification. Conversely, the second criterion is subjective: it determines "personal data" based on the capabilities of the specific entity processing the data. If this entity lacks the necessary information to connect the data to a

[5] Article 4(7) GDPR.
[6] GL par. 25.
[7] GL par. 51.
[8] GL par. 52.

recognizable individual, even if such information exists elsewhere, then that entity is not classified as a data controller under the GDPR. In this case, the data in question would not be deemed "personal data."

The case law of the CJEU in interpreting the notion of personal data is clearly treading towards the subjective criterion. In the Breyer[9] case the CJEU held that the "data" could be considered "personal data" only if the controller itself can link those data to a natural person using additional information possessed by someone else which means that data may be "personal data" for some controllers but not for others[10].

In the Scania case[11] (C- 319/22), the CJEU, where the it had to determine whether Vehicle Identification Numbers (VIN) constitute personal data, held that "*where independent operators may reasonably have at their disposal the means enabling them to link a VIN to an identified or identifiable natural person […] that VIN constitutes personal data for them, within the meaning of Article 4(1) of the GDPR, and, indirectly, for the vehicle manufacturers making it available, even if the VIN is not, in itself, personal data for them*". Again this is another application of the subjective criterion where "data" are "personal data" not for everyone but only for those which are actually able to link those data to an identifiable person.

More recently, in the SRB case[12], in a case initiated by the EDPS, the CJEU dismissed the action of the EDPS stating, *inter alia*, that Deloitte, the SRB's processor, was not in possession of the information necessary to re-identify the authors, natural persons, of some specific comments included in a subset of anonymized data and, therefore, those data had not to be considered "personal data" within the meaning of GDPR. The CJEU stated in the SRB case that the EDPS mistakenly considered the possibility of re-identification only "*from the SRB's perspective and not from Deloitte's*"[13] – again re-affirming that a subjective criterion should be followed and not an objective one.

Finally, in the appeal of the above SRB case, where the final decision has not yet been issued, the AG Spielmann in his opinion held, against the EDPS, that the "*it seems to me disproportionate to impose on an entity, which could not reasonably identify the data subjects, obligations arising from*

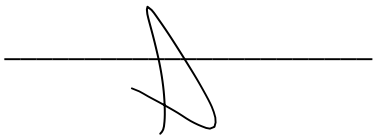
[9] *Ibidem*.
[10] Breyer, above, par. 49 "*having regard to all the foregoing considerations, the answer to the fi rst question is that Article 2(a) of Directive 95/46 must be interpreted as meaning that a dynamic IP address registered by an online media services provider when a person accesses a website that the provider makes accessible to the public constitutes personal data within the meaning of that provision, in relation to that provider, where the latter has the legal means which enable it to identify the data subject with additional data which the internet service provider has about that person*".
[11] C- 319/22.
[12] Case T-557/20.
[13] SRB par. 103.

Regulation 2018/1725, (27) obligations which that entity could not, in theory, comply with or which would specifically require it to attempt to identify the data subjects"[14].

If the case law of the CJEU is clearly heading towards the adoption of the subjective criterion of personal data, the GL should be coherent with the latest case of the Court and, therefore, should take a more nuanced approach in relation to whether metadata, encrypted data or hashed data should be considered to be personal data within the meaning of the GDPR.

In particular, there are various zero-knowledge technologies, widely implemented within blockchains, which allow data to be encrypted in a way where the key to decrypt those data are only in the possession of the data subjects. In such cases, we recommend that the EDPB adopts an approach aligned with the latest CJEU case law, aiming to prevent unnecessary future judicial litigation. This would lead to the conclusion that the data in question should not be classified as "personal data," and consequently, the GDPR would not apply to its processing.

Paolo Maria Gangi LL.M.



[14] SRB appeal Case C-413/23, par 58.