POLITIET
KRIPOS

The National Criminal Investigation Service

European Data Protection Board

Your reference:	Our reference:	Place, date:
Guideline 02/2025	25/128844 - 1	Oslo, 06.09.2025

Feedback on Guideline 02/2025 on processing of personal data through blockchain technologies

Introduction

The Norwegian National Criminal Investigation Service (NCIS), through its National Cybercrime Centre, is the Norwegian police's centre of expertise on cryptocurrency investigations.

Investigative techniques relating to cryptocurrency are rapidly evolving, and are particularly relevant to the investigation of e.g. cybercrime, fraud, organized drug trafficking and CSAM cases. Cryptocurrency services are also being offered by unregulated underground banking and hawala systems, which do not comply with anti-money laundering regulations.

Blockchain technologies raise a number of important and novel questions regarding the processing of personal data. The NCIS therefore welcomes the guidelines on processing of personal data through blockchain technologies, which provide a number of useful clarifications.

As an initial observation, it is unclear to us whether the lack of references to the Directive EU 680/2018 (Law Enforcement Directive or LED) in the guidelines is due to the EDPB not finding the LED relevant in the context of blockchain technologies, or rather to the scope of these particular guidelines being limited to processing under the GDPR. In the former case, we would argue that, for the reasons set out above, processing of blockchain data is quite relevant also under the LED, and we would consequently welcome the inclusion into the guidelines of relevant references to the LED.

Below, we provide our perspectives on the application of the definition of personal data in this context.

KRIPOS
Address: Postboks 2094 Vika, 0125 Oslo / Street address: Nils Hansens vei 25, 0667 Oslo / (+47) 23 20 80 00
kripos@politiet.no / www.politiet.no / Organisation number: 974760827

The application of the concept of "personal data" in the guidelines

As stated in section 3.2 of the guidelines, the application of the concept of personal data in the GDPR – and therefore also in the guidelines – is conditioned on the processing of data which, "by means reasonably likely to be used", can be used to identify individuals. This would be similar under the LED. Here it would be helpful if the guidelines would be somewhat more specific on the question of personal data in the context of blockchains, e.g. when the "risk of identification appears in reality to be insignificant" cf. C-582/14 *Breyer* para 46.

Hereunder, it would be useful if the EDPB would elaborate on the situation mentioned in paragraph 27 in the guidelines regarding approaches providing "ways of hiding identifiers using advanced cryptographic tools, but [where] the data which replaces those identifiers may still constitute personal data". In our experience, the blockchains for cryptocurrencies such as Monero, which utilize several cryptographic techniques (encrypting both the amount transferred, the sender's and the receiver's address and mixing these using ring signatures), would typically not fall under the definition of personal data. This is due to the absence of means reasonably likely to be used to identify the sender or the receiver. Other and even more privacy-preserving cryptocurrencies are also being brought to market.

We would also note that the reference given in section 3.2 to https://defillama.com/hacks may be misleading. The primary purpose of this site is to catalogue stolen values, and it is in our view a poor source of information for personal data breaches.

As for the reference in section 4.9 to cryptanalytically-relevant quantum computers, it would constitute a high bar indeed if this emerging, uncertain, and currently undeployed technology should be brought into the assessment of whether certain data should be considered as personal data.

Conclusion

The NCIS welcomes guidelines 02/25 and suggests that references to the LED are included as appropriate, and that the concept of "personal data" as applied to blockchain technologies is further elaborated on. This elaboration should be made bearing in mind that some blockchain technologies are deliberately engineered to provide anonymity, and recognizing that the definition of personal data is not all-encompassing.

Yours sincerely

Laila Søndrol
Assistant Chief of Police

The document has been signed electronically.