Lexify Insights

YOUR TRUSTED LEGAL NEWSLETTER

DATA PROTECTION FOR BLOCKCHAIN TECHNOLOGIES

Technology & Digital Assets | 03/2025

LEXIFY
MORE THAN LAWYERS

Introduction

The European Data Protection Board ("EDPB") has issued crucial Guidelines 02/2025 (hereinafter the "Guidelines"), providing a much-needed framework for organizations leveraging blockchain or Distributed Ledger Technologies ("DLTs") while processing personal data. As legal practitioners and operators within the rapidly evolving blockchain sector, understanding and implementing these Guidelines is not merely advisable but essential for ensuring not only compliance with the General Data Protection Regulation ("Regulation (EU) 2016/679 or "GDPR") but most of the principles could be similarly extended to the Swiss Federal Act on Data Protection ("FADP").

Blockchain Fundamentals, Swiss FADP and GDPR Interplay

The Guidelines first establish a common understanding of blockchain technology[1], encompassing components like block data structure (e.g. accounts, smart contract storage, receipt logs etc.), consensus algorithms (e.g., Proof-of-Work, Proof-of-Stake), governance mechanisms, communication networks, associated ecosystems (wallets, block explorers), as well as off-chain storage.

A critical distinction is made between blockchain natures:

- permissionless vs. permissioned: permissionless blockchains (e.g., Bitcoin, Ethereum) allow anyone to participate, read, and write, posing greater challenges for control and responsibility assignment. Permissioned blockchains restrict participation to authorized entities, offering clearer governance and responsibility allocation, which the EDPB strongly encourages organizations to favor unless well-justified reasons dictate otherwise. If permissioned models are infeasible, organizations must question if blockchain is appropriate at all; and
- public vs. private: public access blockchains necessitate careful consideration under Article 25 GDPR and Article 7 FADP (Privacy by design and by default), which requires that personal data not be made accessible to an indefinite number of persons without the data subject's intervention.

The choice of blockchain architecture (permissioned vs. permissionless, public vs. private) is a fundamental compliance decision.

[1] Blockchain allows data is replicated by multiple participants peer-to-peer and so stored in multiple locations; validation of data added to database that does not need the endorsement of a central counterparty; any update or removal of validated data can be detected; and access to data is available to all participants. See the Guidelines, p. 5.

Operators must document the rationale for their choice, demonstrating why a specific blockchain type is necessary and proportionate for the intended processing purpose, especially if opting for a public and/or permissionless model.

Switzerland's FADP shares fundamental principles with GDPR (lawfulness, transparency, purpose limitation, minimisation, accuracy, security, data subject rights and cross-border transfer rules). The challenges identified by the EDPB regarding blockchain's immutability versus erasure/rectification rights, responsibility allocation, and the need for specific technical and organizational measures may be directly applicable to entities processing personal data of Swiss residents under the FADP. The solutions and risk mitigation strategies outlined in the EDPB Guidelines provide relevant practical guidance for achieving FADP compliance in a blockchain context.

Personal Data within the Blockchain Ecosystem

Personal data can exist both on-chain and off-chain:

- on-chain data: this includes transaction metadata[2] (e.g., public keys/addresses of participants, which qualify as personal data if linkable to an individual) and the transaction payload (content data, which might contain personal data relating to participants or third parties). Other on-chain data structures like smart contract storage can also hold personal data; and
- off-chain data: data stored outside the blockchain, potentially linked via on-chain references. Additionally, data processed when interacting with the blockchain (e.g., IP addresses via dApps or wallets) but not stored on-chain is also relevant.

The Guidelines strongly discourage storing personal data in plain text on the blockchain due to conflicts with Article 5 GDPR or Article 6 Swiss Federal Act on Data protection principles. Data directly identifying individuals could be critical due to the practical impossibility of deletion or modification in most implementations.

Where personal data processing on-chain is deemed unavoidable after rigorous necessity/proportionality assessment, the Guidelines discuss techniques, while acknowledging their limitations:

1. encryption: encrypting data before on-chain storage limits access to keyholders;
2. hashing: storing only a salted or keyed hash on-chain, with the original data and secret key/salt kept securely off-chain. The hash itself remains personal data. Deleting the off-chain key/salt can break the link, subject to similar caveats as encryption regarding key compromise and algorithm security. This necessitates secure off-chain processing;
3. cryptographic commitments: storing a commitment on-chain allows proving data integrity later without revealing the data initially. Deleting the original data and its 'witness' (off-chain) can render the on-chain commitment useless for identification, assuming a perfectly hiding scheme;
4. off-chain storage with on-chain anchors: the preferred approach is often to store actual personal data off-chain, placing only pointers, commitments, or keyed hashes on-chain to act as proofs of existence or integrity anchors; and

[2] Public keys can be used to identify individuals by means reasonably likely to be used, for example in case of data breach. See the Guidelines, p. 8.

5. practical Implication: operators must prioritize off-chain storage for personal data. If on-chain storage is strictly necessary, employ state-of-the-art techniques like keyed hashing or commitments, coupled with robust off-chain security and key management. Operators should document the chosen method and risk assessment as well as establish that plain text storage shall be avoided.

Roles and Responsibilities: Controller & Processor Determination

Assigning roles under GDPR and Swiss FADP data controller, data processor is complex in decentralized systems. The technological setup does not absolve actors of responsibility. A factual assessment considering the governance mechanism, technical features, and relationships between actors is required.

- Permissioned Blockchains: typically have clearer governance, often with an authority (single or group) granting participation rights. This authority often determines purposes and means, likely qualifying as a controller or joint controller.
- Permissionless Blockchains: responsibility is harder to pinpoint. Their role varies. If nodes merely execute technical validation based on predefined rules without determining purposes/means, they might not be controllers. However, if they process data on behalf of a controller, they could be processors (i.e. data processing agreement required). Crucially, if nodes (individually or collectively) exercise decisive influence over purposes and essential means (e.g., choosing transactions for a block, deciding on protocol forks), they may qualify as controllers or joint controllers. The EDPB encourages the establishment of legal entities (e.g., consortia) for nodes in such scenarios to act as the controller.

Swiss FADP and GDPR Principles & Blockchain Challenges

Applying Article 5 principles requires careful consideration:

- processing needs a valid legal basis. Consent could be problematic if withdrawal cannot be effectively implemented (i.e., data cannot be erased/anonymized). Legitimate interests require careful balancing. Transparency requires clear information to data subjects *before* data submission. Fairness prohibits unexpected or detrimental processing.
- purposes must be specified, explicit, and legitimate. The disintermediated nature can complicate ensuring data isn't used for incompatible purposes by participants.
- process only necessary data, minimize on-chain footprint and accessibility using techniques discussed earlier.
- emphasizes the need for accuracy *before* data submission. Rectification mechanisms are discussed below.
- data must not be kept longer than necessary. The blockchain's lifetime is generally *not* an appropriate retention period. Requires by design solutions allowing effective erasure or anonymization (e.g., deleting off-chain data/keys linked to on-chain hashes/commitments, rendering the on-chain data non-personal). If effective erasure/anonymization is impossible for the required retention period, personal data should not be stored on that chain. Justification is needed if retention equals blockchain lifetime.
- Integrity and Confidentiality: Blockchain inherently provides integrity via cryptography and consensus. Confidentiality, however,

requires active measures: permissioning access, encrypting payloads, securing off-chain data and keys, managing participant trustworthiness.

Data Subject Rights Implementation

Facilitating data subject rights is mandatory and technology-neutral.

- Access and portability: generally feasible with appropriate mechanisms for providing information and data extracts.
- Rectification and erasure: the most challenging rights due to immutability are:
  1. erasure: direct deletion is often technically impracticable or undermines the blockchain's integrity. Compliance must be achieved by rendering personal data effectively anonymous. This relies heavily on the techniques discussed: storing minimal data on-chain (e.g., keyed hashes, commitments) and ensuring that deleting associated off-chain data (original data, keys, salts) breaks the linkability to the data subject using means reasonably likely to be used.
  2. rectification: may sometimes be achieved by adding a new transaction that invalidates or corrects a previous one (leaving the original intact but marked as superseded).
- automated decision-making: if smart contracts result in solely automated decisions with legal or similarly significant effects, safeguards shall apply (right to human intervention, express point of view, contest decision). This must be possible even for post-execution situations.

Conclusion

At Lexify, we are one of the first law firms specializing in review compliance associated with blockchain technology and crypto-assets, uniquely positioned to guide businesses and individuals in navigating these legal frameworks. Navigating the intersection of blockchain and data protection requires a proactive, risk-based, and design-led approach. The Guidelines serve as an indispensable map for legal and technical practitioners aiming to innovate responsibly within the bounds of Swiss and European laws. Our expertise ensures your operations remain compliant and protected from regulatory risks, safeguarding your success.

Contact

Connect with us

Thank you for taking the time to read our article. We hope you found it informative and engaging. If you have any questions, feedback, or would like to explore our services further, we're here to assist you.

Contact Information

For inquiries about our legal assistance, please contact:

- Email: Emanuele.gambula@lexify.io
- Phone: +41 76 232 66 83

Follow Us

Stay updated and connected with us on social media for the latest news, insights, and updates:

- LinkedIn: Lexify

Explore More

Visit our website to discover more about our products, services, and the solutions we offer at https://www.lexify.io/

Our Team

Emanuele Gambula
☎ +41 76 232 66 83
✉ emanuele.gambula@lexify.io

Alberto Borri
☎ +41 77 461 38 47
✉ alberto.borri@lexify.io