Blockchain and Data Protection

Tensions between blockchain technology and data protection principles

Dr. Matthias Artzt (CIPP/E)
Senior Legal Counsel, Group Data Privacy, Deutsche Bank AG,
Frankfurt am Main
1. Allocation of roles and responsibilities under the GDPR
2. Data subject rights under the GDPR
3. Principles of purpose limitation and data minimization vs blockchain finality
4. Techniques to mitigate data protection risks
Agenda (2/2)

5. Data Privacy Impact Assessment
6. Privacy by Design
7. Legal grounds under the GDPR
8. Take aways
1. Allocation of roles and responsibilities (1/8)

1. Exhaustive list of roles under the GDPR:
   - (Joint) controller, Art. 4 (7), Art. 26: „natural or legal person (...) which, alone or jointly with others, determines the purposes and means of the processing of personal data (...)“ > similar to „business“ under CCPA
   - Processor, Art. 4 (8): „natural or legal person (...) which processes personal data on behalf of the controller“ > similar to „service provider“ under CCPA

2. The usual players in a blockchain environment:
   - Miners
   - Nodes
   - Wallets
   - Users
   - Developers of smart contracts
   - Oracles
   - Governance bodies
1. Miners

- **Definition:**
  - Mining is the act of solving a mathematic puzzle within the proof of consensus model based on the protocol as defined in the blockchain software (NIST)
  - Miners validate transactions to be added to the blockchain

- **Legal implication:**
  - Miners ≠ controllers ►not determine the specific purpose of any data processing activity
  - Miners ≠ processors ►not carry out specific services based on instructions of the controllers

Note: The blockchain protocol doesn’t contain instructions as to how to deal with personal data written on a blockchain
1. Allocation of roles and responsibilities (3/8)

2. Nodes
   • Definition:
     • Nodes are the decentralized computers that store a copy of the blockchain
     • Storing is an IT operation and cannot be linked to a decision-making process (controller)
   • Legal implication:
     • Nodes ≠ controllers ≠ processors ► using the blockchain technology and participating in the blockchain network cannot be interpreted as a determination of the means and the purpose of a specific data processing activity ► belong to blockchain infrastructure
1. Allocation of roles and responsibilities (4/8)

3. Wallets

• Definition:

  • Wallets are software packages at the application level designed to store and manage asymmetric keys and addresses used for transactions (NIST)
  • Allow blockchain users to control their own private key and to interact with the blockchain network by sending transactions to miners for validation purposes

• Legal implication:

  • Wallets ≠ controllers ≠ processors ► wallets are only the vehicle to pass data to miners ► this happens under the control of the blockchain users
1. Allocation of roles and responsibilities (5/8)

4. Users
   • Definition:
     • Participate in any transaction in a blockchain network provided that such transaction stores or processes personal data
     • CNIL: User = controller when (i) the user is a natural person; and (ii) the processing is related to a professional or commercial activity; or, when the user is a legal person that submits personal data to a blockchain
     • EU Blockchain Observatory: User = controller when the user submits personal data to the blockchain as part of his business activity
   • Legal implication:
     • Delineation from the household exemption of Art. 2 (2c) of the GDPR
       ► household/private activity ► GDPR doesn’t apply ► user ≠ controller
5. Developers of smart contracts

• Definition:
  • Smart contract is a piece of software that, once deployed to a blockchain network, may be executed independently from their developer when called by a blockchain user
  • Developer creates an algorithm to be built in the software

• Legal implication:
  • CNIL: Developer has no role to play unless he intervenes in the data processing actively
  • Developer only provide a software solution to blockchain users and don’t operate that software while blockchain users write personal data to the blockchain leveraging the algorithm of the smart contract
  • Developer ≠ controller ≠ processor
6. Oracles
   • **Definition:**
     * Oracles are agents that allow the transfer of external data feeds to the blockchain leveraging smart contracts
     * Necessary to process external real-world events to be inputted onto the blockchain for further usage
     * Oracles have a strong influence on the data processing operation and its result carried out by the smart contract algorithm
   
   • **Legal implication:**
     * Oracles = controller if they have a commercial interest in the related data processing and the outcome of that data processing activity
     * Requires case-by-case consideration
     * Rule of thumb: Oracles belong to blockchain infrastructure
1. Allocation of roles and responsibilities (8/8)

7. Governance bodies
   - **Definition:**
     - Only applicable in private blockchains
     - Group of natural persons and/or legal entities tasked with monitoring blockchain transactions
     - Defining the roles of the participants upfront
   
   - **Legal implication:**
     - Governance body = controller if it has control over the processing of personal data by determining its purpose and means (usage of smart contract algorithms)
     - Governance body may determine one participant to act as controller provided that participant is empowered to make decisions on behalf of the group. Other group members = processor or (joint-/co) controllers
2. Data subject rights under the GDPR (1/3)

1. How do data subject rights apply to the blockchain?
   a) Applicability of the GDPR
      • Once one block contains personal data and the block is added to the blockchain ► storage = data processing pursuant to Art. 4 sec. 2 of the GDPR
      • Data subject may exercise his rights pursuant to Art. 15 – 22 of the GDPR. Problem: against whom?
   b) Distinction between public and private blockchains in relation to enforcing data subject rights
      • Private blockchains: Governance body to be the first choice to address any data subject rights. Joint controllers according to Art. 26 of the GDPR
      • Public blockchains: Data subjects face a challenge to (i) identify the controller, and to (ii) get the controller to carry out his obligations
2. Data subject rights under the GDPR (2/3)

2. Factual enforceability of particular data subject rights

a) Right to access personal data, Art. 15 GDPR
   - Basic right: prerequisite for the exercise of any other right under the GDPR
   - Necessary to understand which data is being processed and for what purpose
   - **Problem**: In a public blockchain a controller, once identified, is factually unable to access data submitted to the blockchain: data is typically encrypted or hashed; impossible to determine whether the related data is personal and relates to the data subject concerned

b) Right to rectify personal data, Art. 16 GDPR
   - Right to request rectification of inaccurate personal data and to complete personal data which is incomplete
   - **Problem**: Impossibility to modify data registered onto a blockchain
2. Data subject rights under the GDPR (3/3)

c) Right to erasure („right to be forgotten“), Art. 17 GDPR

• What does erasure mean?
  • Data subject may request the erasure of his/her personal data provided one of the conditions set out in Art. 17 sec. 1 GDPR applies
  • Erasure as a legal term is defined very broadly (e.g. expunge, overwriting, making data unusable)
  • Problem: Impossibility to delete data once registered onto the blockchain
  • But: This is not a Catch 22 situation since alternative solutions are permissible when the erasure is virtually not viable ►see techniques to mitigate data protection risks
3. **Principles of purpose limitation and data minimization vs blockchain finality (1/3)**

- **Principle of purpose limitation of data processing**
- **Principle of data minimization**
- **Immutability of information being submitted to the blockchain (blockchain finality)**
3. Principles of purpose limitation and data minimization vs blockchain finality (2/3)

1. Principle of purpose limitation
   • Definition:
     • “Personal data shall be collected for specific, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes” (Art. 5 sec. 1b GDPR) and “A business shall not (…) use personal information collected for additional purposes without providing the consumer with notice consistent with this section” (sec. 1798.100 (b) CCPA)
     • Purpose limitation is the “cornerstone of data protection” (Art. 29 Data Protection Working Party [now: EDPB])
   • Legal implication on blockchain:
     • Blockchain, by nature, continuously processes data by storing it onto the blockchain which also includes legacy personal data (data which is not needed any more, e.g. after completion of a particular transaction)
2. Principle of data minimization

- **Definition:**
  - Only those data which is necessary to meet the purpose determined by the controller must be collected and processed.
  - Period for which the personal data is being stored must be limited to a strict minimum (Recital 39 of the GDPR).

- **Legal implication on blockchain:**
  - Blockchain artefacts clash with the data minimization principle:
    - Ever-growing nature of databases containing personal data
    - Replication of data in a blockchain network where each node stores a full copy of the database
4. Techniques to mitigate data protection risks (1/5)

Assessment of the permissibility of submitting personal data to the blockchain:

- Is it inevitable to store personal data on a blockchain?
- Private blockchain first choice
- Usage of innovative techniques
4. Techniques to mitigate data protection risks (2/5)

- **Big picture**: How is the data being processed and is there any need to store it on a blockchain? Offchain storage should be the first choice
- **Usage of private blockchains as primary objective**
- **Usage of innovative encryption techniques**, particularly with regard to public blockchains:
  - Anonymization as primary approach
  - If anonymization is not doable, **state-of-the-art encryption, particularly hashing**
  - Please note: Hashing is an encryption technique and does not entail anonymization ► Hashing does not turn personal data into non personal data ► GDPR applies
4. Techniques to mitigate data protection risks (3/5)

- **Usage of interoperable blockchains („multi-layered“)**
  - **Challenge:** Reconciling the storage of personal data which is not needed any more („legacy data“) and the principles of purpose limitation and data minimization
  - **Removing legacy data from a private blockchain and transferring it to a public blockchain**
  - Both blockchains are intertwined: the public blockchain links to the private blockchain
    - For real time data processing: private blockchain
    - For legacy data: public blockchain
  - **Problem:** Legacy data remain on the public blockchain ► data is being replicated and still visible
  - **Result:** Good instrument for safeguarding personal data, but not in line with the principles of purpose limitation and data minimization
4. Techniques to mitigate data protection risks (4/5)

- **Off-chain storage and hashing of legacy data („hashing-out“)**
  - **Challenge:** Reconciling the storage of legacy data and the principles of purpose limitation and data minimization
  - **Removing legacy data from the blockchain and storing it in an external off-chain database; linking personal data via hash point**
  - **Hashes of the personal data being put off-chain remain onto the blockchain**
  - **Problem:** Hash remains on the blockchain and still qualifies as personal data
    - GDPR applies to on-chain hash values
    - Does hashing-out resolve the issue around the above principles and erasure requests?
4. Techniques to mitigate data protection risks (5/5)

• Erasure of personal data by deleting off-chain legacy data
  • Hashing-out and deleting legacy data comply with an erasure request even though the hash of the personal data remains on the blockchain
  • Rationale: ► The on-chain hash has nothing to relate to as soon as the corresponding personal data on the external off-chain database has been deleted; the hash becomes a random string with no meaning
    ► A cryptographic hash function is a „one-way function“: it is not possible to recreate or reverse engineer the original data from the hash function
    ► Deletion of the off-chain legacy/reference data changes the legal nature of the hash value from personal data to non personal data
  • Result: Hashing-out is a technique to comply with the principles of purpose limitation and data minimization as well as with erasure requests
Definition and impact on controllers

- Controller has to carry out a DPIA pursuant to Art. 35 GDPR prior to the data processing operation if
  - new technologies are used
  - processing is likely to result in a high risk to the rights and freedoms of data subjects
- DPIA involves balancing the interests of the data controller against those of the data subjects, in particular:
  - description of the data processing and the purpose(s)
  - assessment of the necessity and proportionality of the processing in relation to the purpose
  - an assessment of the risks to the data subjects
  - the measures in place to address the risk identified
1. Definition and impact on controllers

- CCPA and GDPR require businesses to adopt security protocols appropriate to safeguard collected personal information
- Art. 25 GDPR more specifically requires controllers to establish appropriate technical and organizational measures to implement data protection principles and to safeguard the rights of data subjects
  ▶ controller must choose that technology from the outset with the least impact on the rights of data subjects
  ▶ privacy considerations must be factored in at the earliest possible stage
  ▶ controller has to implement measures to ensure minimization of the data to be processed as well as security (e.g. pseudonymization, encryption)
2. Legal implication on blockchain

- Controller should follow the sequence of assessing the permissibility of submitting personal data to the blockchain (see chart above)
- Usage of state-of-the-art encryption techniques whenever on-chain storage of personal data is inevitable (ultima ratio!)
  ▶ controller should register personal data and hash or, at least, encrypt the data (CNIL as of Nov 6, 2018)

3. Potential use cases in the industry

- **Health sector:** Record and authenticate medical data and customize its use for other parties (e.g. personalized medicine, data sharing for public health research) ▶ dealing with sensitive (health) data implies that strong privacy mechanisms must be put in place ▶ need to conduct both DPDD and DPIA
- **Crypto currencies:** Adding additional layers of privacy to the transactional information (identity of blockchain users is obfuscated)
7. **Legal grounds under the GDPR**

1. **Contractual necessity, Art. 6 (1)(b) GDPR**
   - Processing necessary for the performance of a contract
   - Relevant regarding smart contracts

2. **Consent, Art. 6 (1)(a) GDPR**
   - Data subject has given consent to the processing of his or her data for one or more specific purposes
   - Consent can be withdrawn by the data subject at any time
   - Unclear to whom the user must give consent in a blockchain context

3. **Legitimate interest, Art. 6 (1)(f) GDPR**
   - Processing necessary for the purposes of the legitimate interests pursued by the controller or by a third party
   - Submitting of personal data to a blockchain is legitimate if, e.g., the processing activity aims to prevent frauds (Recital 47 of the GDPR)

4. **Compliance with legal obligation, Art. 6 (1)(c) GDPR and public interest, Art. 6 (1)(e) GDPR**
8. Key Take Aways

- It is just technology
- Law is technology neutral
- Tensions with GDPR can be overcome
- Usage of state-of-the-art encryption is key
- Carry out PIA and DPDD
- Private blockchain first
- Track guidance of data protection authorities
Question & Answer
Thank you!

Contact us:
info@fpf.org
@FutureofPrivacy
www.fpf.org/classes