Blockchain & GDPR

IRIS 2026, 20.2.2026, Salzburg

Dr. Jörn Erbguth, Diplom Jurist und Diplom Informatiker, Berater Blockchain & GDPR, Universität Genf
Olga Stepanova, LL.M. (Berkeley), Rechtsanwältin, Partnerin ByteLaw Rechtsanwälte
Michael Kissler, LL.M. (Warschau), LL.M. (Nottingham), Rechtsanwalt, Winheller Rechtsanwälte

Blockchain & GDPR

16:05	Kurze **Einführung** in Blockchain-Technologie, typische Einsatzgebiete und Konfliktfelder mit der DSGVO	Olga Stepanova
16:25	**Definition personenbezogener Daten**; Problematik der weiten Auslegung des EDSA beim Einsatz privacy-preserving technologies; Einordnung von EDPS v. SRB sowie des Omnibus-Vorschlags der EU-Kommission	Jörn Erbguth
16:45	**Electronic Ledgers nach eIDAS** einschließlich der Implementing Acts; Anforderungen an Integrität und Unveränderbarkeit	Jörn Erbguth
16:50	**Drittstaatentransfers** im Kontext der Veröffentlichung im Internet; Anwendbarkeit der Lindqvist-Rechtsprechung auf Public Permissionless Blockchains	Olga Stepanova
16:55	**Financial- und Crypto-Regulierung** und ihr Spannungsverhältnis zur DSGVO	Michael Kissler
17:15	Diskussion	

Definition personenbezogener Daten

- Problematik der weiten Auslegung des EDSA beim Einsatz privacy-preserving technologies

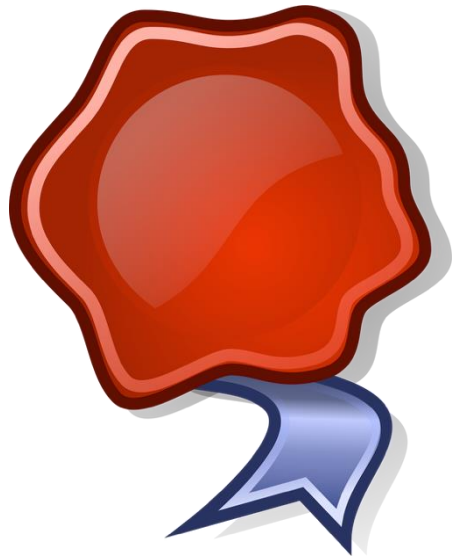
- Einordnung von EDPS v. SRB sowie des Omnibus-Vorschlags der EU-Kommission

Öffentliche Verifizierungsartefakte

Dokument ist nicht öffentlich

Dokument enthält personenbezogene Daten

Bestätigung ist öffentlich



- Bestätigung ohne das Dokument erlaubt keine Rückschlüsse
- Bestätigung bestätigt nur, was im Dokument enthalten ist und enthält keine weitere Information

Öffentliche Verifizierungsartefakte

Perfectly hiding commitments

- Z.B. Hashwerte, richtig eingesetzt

Zero Knowledge Proofs

- Beweis: Alter > 18 Jahre, ohne Offenlegung des Alters
- Beweis: Habe mindestens x Coins in meinem Account, ohne Offenlegung des Kontostandes

EDSA: Hashes seien personenbezogene Daten

52. **Hashing of personal data:** Another measure is to store only a salted or keyed hash of the personal data on the blockchain. The unhashed data itself, as well as the secret key or the long random salt used, are stored confidentially off the chain. Although this may be referred to as "off chain" storage, 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. The advantage of this architecture is that the original data (i.e. the argument of the hash function) cannot easily be recovered from the hash. Indeed, a hash obtained through a state-of-the-art hash function and a randomly generated secret key or salt of a sufficient size, will, in theory, be verifiable only by people having access to the original data and the given associated key or salt. This also means that, after deletion of the secret key or salt, the hash should not be linkable to the original data, provided that the algorithm has not been broken, the keys have not been compromised or leaked, and the salt was not leaked or poorly chosen. However, this architecture requires the use of another system in order to store the data itself, therefore creating a personal data processing in another component of the infrastructure, which bears its own risk. It should also be noted that the use of unsalted or unkeyed hashes should, in general, not be considered sufficient to guarantee the necessary level of confidentiality protection for storing personal data on a public blockchain.

Vergleich mit eIDAS-Zertifikaten

Laut EDSA Zertifikat kein personenbezogenes Datum

Öffentliches, qualifiziert elektronisches Zertifikat, gibt keine Information über das Dokument, ermöglicht aber die Verifikation

Personenbezogene Daten

Dokument mit personenbezogenen Daten
Signiert durch ein qualifiziertes elektronisches Siegel

Laut EDSA Commitment sei personenbezogenes Datum

Personenbezogene Daten

Perfectly hiding commitment, z.B. ein Hashwert, gibt keine Information über das Dokument, ermöglicht aber die Verifikation

Dokument mit personenbezogenen Daten
Signiert durch eine einfache elektronische Signatur

Definition personenbezogener Daten

- Identifizierbarkeit durch wen?
- Information
- Risikobasiert (means reasonably likely to be used)

Art. 4 Nr. 1 DSGVO

„personenbezogene Daten“ alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen

Erwägungsgrund 26 DSGVO

To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly.

Identifizierbarkeit durch wen?

- Keine allgemeine Identifizierbarkeit
- Identifizierbar nur duch die, die das verifizierte Dokument haben
- Bei relativer Definition, ist es für diejenigen kein personenbezogenes Datum, die das Dokument nicht haben

EDPS v SRB und Digital Omnibus

Information

- Die Information des Dokumentes ist nicht im Verifizierungsartefakt
- Ist die Verifizierbarkeit des Dokumentes eine Information, die sich indirekt auf die Personen bezieht, auf die das Dokument sich bezieht?

Stellt die Verifizierbarkeit eine eigene Information dar?

Das Verifizierungsartefakt ermöglicht nur die Verifizierung der einfachen elektronischen Signatur, sie ist keine zusätzliche Bestätigung Dritter!

Risikobasiert (reasonably likely)

Keine personenbezogenen Daten wenn die Identifizierung:

- unverhältnismässiger Aufwand
- gesetzlich verboten
- praktisch nicht durchführbar
- ohne Interesse, da die Informationen bereits bekannt ist?

Wenn diejenigen, die Informationen mit Personen identifizieren können, diese Information bereits haben, gibt es kein Risiko der Identifizierung

Ausnahmen

- Hashwerte als Index für weitere Information

  Mit dem Hashwert des Dokumentes können weitere Informationen zum Dokument verbunden werden, z.B. ein Widerruf, neuere Dokumente, Detaildaten etc.

- Hashwerte als unabhängige Äusserung über ein Dokument

  Dritte bestätigen, dass die Inhalte des Dokumentes zutreffen oder fehlerhaft seien.

Ergebnis

Sind Verifzierungsartefake personenbezogene Daten?

Identifizierbarkeit? ⛔

Nur eingeschränkt (relativer Personenbezug)

Information? ⛔

Die Information befindet sich im Dokument und wird allenfalls gespiegelt

Risiko? ⛔

Eine Identifizierung ist nach allgemeinem Ermessen unwahrscheinlich, wenn die Information denjenigen, die die Identifizierung vornehmen können, bereits haben.

https://www.blockchain4europe.eu/wp-content/uploads/2025/12/BC4EU-Report-Blockchain-and-the-GDPR.pdf

Electronic Ledgers (elektronische Journale) nach eIDAS

ABSCHNITT 11

elektronische journale

Artikel 45k

Rechtswirkungen elektronischer Journale

(1) Einem elektronischen Journal darf die Rechtswirkung oder die Zulässigkeit als Beweismittel in Gerichtsverfahren nicht allein deshalb abgesprochen werden, weil es in elektronischer Form vorliegt oder die Anforderungen an qualifizierte elektronische Journale nicht erfüllt.

(2) Für Datensätze in einem qualifizierten elektronischen Journal gilt die Vermutung der eindeutigen und genauen fortlaufenden chronologischen Reihenfolge und der Unversehrtheit.

Artikel 45l

Anforderungen an qualifizierte elektronische Journale

(1) Qualifizierte elektronische Journale müssen folgende Anforderungen erfüllen:

a) sie werden von einem oder mehreren qualifizierten Vertrauensdiensteanbietern erstellt und verwaltet;

b) sie stellen die Herkunft der Datensätze im Journal fest;

c) sie gewährleisten die eindeutige fortlaufende chronologische Reihenfolge der Datensätze im Journal;

d) sie zeichnen die Daten so auf, dass jede spätere Änderung an den Daten sofort erkennbar ist, und gewährleisten somit ihre Unversehrtheit im Zeitverlauf.

(2) Bei einem elektronischen Journal, das den in Absatz 3 genannten Standards, Spezifikationen und Verfahren entspricht, wird davon ausgegangen, dass es die Anforderungen des Absatzes 1 erfüllt.

(3) Bis zum 21. Mai 2025 erstellt die Kommission im Wege von Durchführungsrechtsakten eine Liste von Referenzstandards und legt, sofern erforderlich, die Spezifikationen und Verfahren für qualifizierte Validierungsdienste nach Absatz 1 des vorliegenden Artikels fest. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

Definition electronic ledgers (elektronischer Journale)

Art. 3 Nr. 52 eIDAS

„Elektronisches Journal“ ist eine Abfolge von Aufzeichnungen elektronischer Daten, die die Unversehrtheit dieser Aufzeichnungen und die Richtigkeit ihrer chronologischen Reihenfolge gewährleistet.

Durchführungsverordnung (EU) 2025/2531 (16.12.2025)

Qualifizierte elektronische Journale müssen gewährleisten:

- Unversehrtheit (Integrity)
- Endgültigkeit (Finality)

Konsensmechanismus, der die Endgültigkeit und Unversehrtheit der im Journal gespeicherten Datensätze und Transaktionen gewährleistet, einschließlich etwaiger Pufferzeiten, bis die Endgültigkeit und Unversehrtheit feststehen

Finality und Immutability

Entwurfsfassung

1. For the purposes of this Regulation, the following definitions apply:

   (a) ‘finality’ means the state of a data record of an electronic ledger wherein it has become irreversible and cannot be modified or removed;

   (b) ‘immutability’ means the property of an electronic ledger wherein data records cannot be modified or removed once added to that electronic ledger;

   (c) ‘distributed electronic ledger’ means an electronic ledger that is shared across a set of distributed electronic ledger nodes and which is synchronized between the distributed electronic ledger nodes using a consensus mechanism;

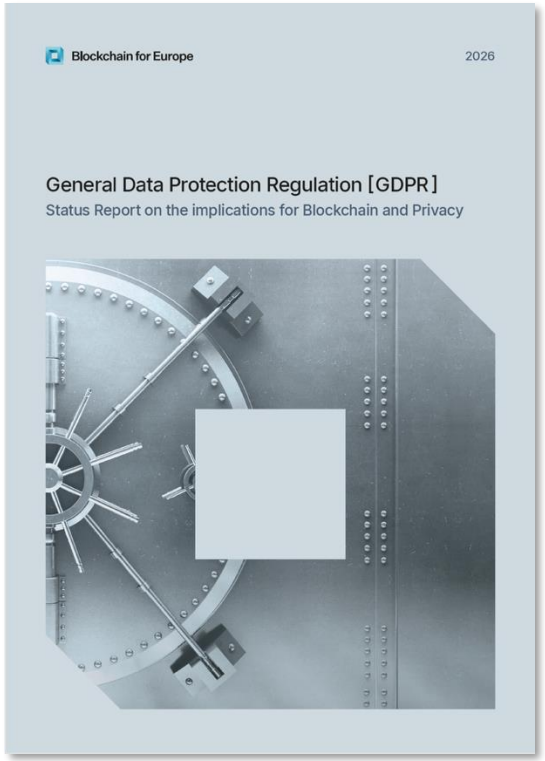
Verabschiedete Fassung

1. For the purposes of this Regulation, the following definitions apply:

(a) ‘finality’ means the state of a data record of an electronic ledger wherein it has become irreversible and cannot be modified or removed;

(b) ‘distributed electronic ledger’ means an electronic ledger that is shared across a set of distributed electronic ledger nodes and which is synchronized between the distributed electronic ledger nodes using a consensus mechanism;

Vielen Dank für Ihre Aufmerksamkeit!



https://www.blockchain4europe.eu/wp-content/uploads/2025/12/BC4EU-Report-Blockchain-and-the-GDPR.pdf