RECHT-TESTBED

Datenschutzrechtliche Aspekte von private Blockchains

Jonas Baumann

Internationales Rechtsinformatik Symposium 2021, 25.2.2021

Gefördert durch:

Bundesministerium für Wirtschaft und Energie

aufgrund eines Beschlusses des Deutschen Bundestages

Fraunhofer

INSTITUT FÜR RECHTSINFORMATIK
UNIVERSITÄT DES SAARLANDES

hgi Horst Görtz Institut für IT-Sicherheit

Agenda

I. Einleitung
II. Die Anwendbarkeit der DS-GVO
III. Datenschutzrechtliche Verantwortlichkeit
IV. Legitimation von Datenverarbeitungen
V. Blockchain & Betroffenenrechte
VI. Fazit

Einleitung

Einleitung

Blockchain-Technologie als datenschutzrechtliche Herausforderung

- Dezentrale Netzwerkstruktur
- Diverse Rollen der Netzwerkteilnehmer
- Unveränderlichkeit der gespeicherten Information
- Einsatz kryptographischer Verfahren
- Verschiedene Netzwerkkonzeptionen
  - Private/public
  - Permissioned/permissionless

Normative Anreize zur Datenschutz-Compliance unter der DS-GVO

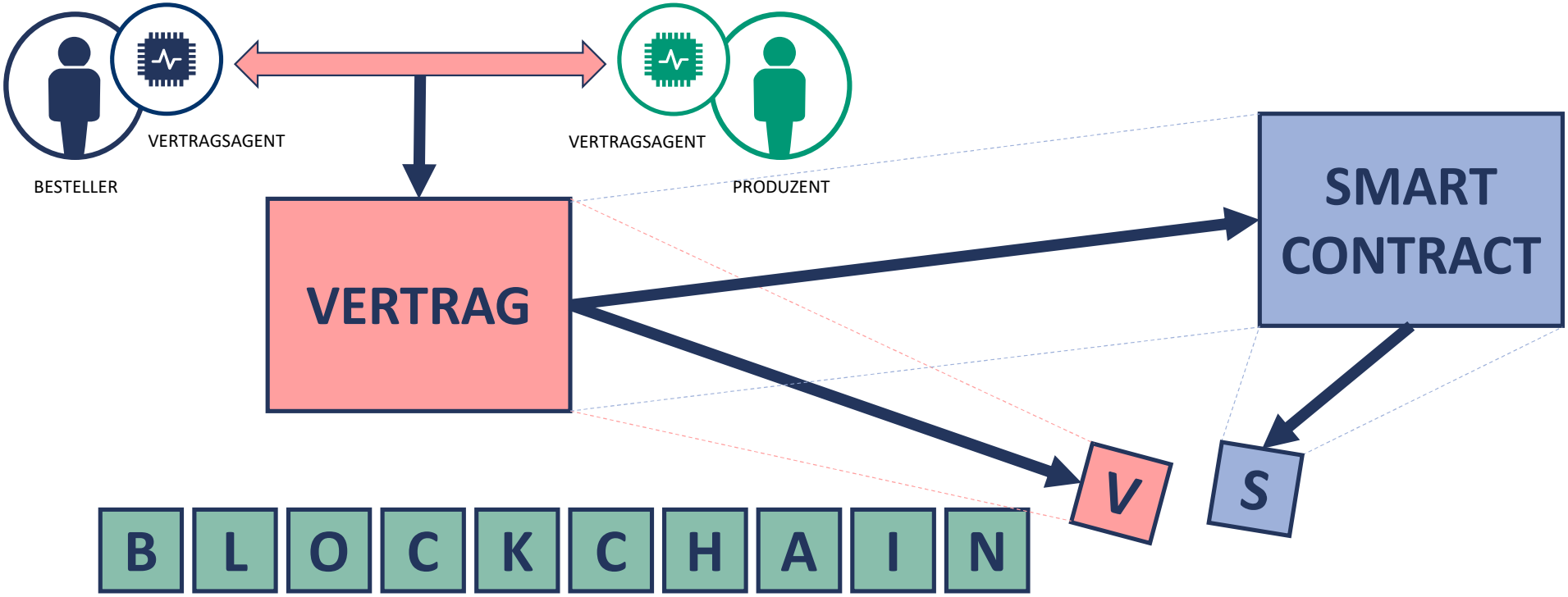
- Bußgelder
- Behördliche Anordnungen
- Zivilrechtliche Haftung

Blockchain-Technologie in der Industrie 4.0

- Dokumentation von Informationen
  - Beweismittel in gerichtlichen Verfahren
  - Blockchainbasierte Register

- Ausführungsumgebung für smart contracts
  - Technische Grundlage automatisierter Vertragsvollziehung

Technische Realisierung von automatisierten Verträgen



RECHT-TESTBED

Eigenschaften von private Blockchains

- Zugang zum Netzwerk wird durch eine zentrale Stelle administriert
- Zugang unterliegt bestimmten Bedingungen
  - Identifikation
  - „Nutzungs- und Teilnahmebedingungen“
  - Rechtemanagement

- Gewisse „Intermediatisierung“ durch die Rolle der zentralen Stelle

Vorteile von private Blockchains

- Sicherheit
  - Beschränkter Zugang
  - Beschränkte Lese- und Schreibrechte
- Privacy
  - Keine öffentliche Transparenz
- Performance
- Flexibilität
  - Konzeption des Netzwerks
  - Anpassung der Netzwerkregeln

Die Anwendbarkeit der DS-GVO

RECHT-TESTBED

Der materielle Anwendungsbereich der DS-GVO

Art. 2 Abs. 1 DS-GVO

„Diese Verordnung gilt für die **ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten** sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.“

Die Auslegung des Begriffs „personenbezogener Daten“

Art. 4 Nr. 1 DS-GVO

„‘personenbezogene Daten‘ [sind] alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.“

RECHT-TESTBED

Die Auslegung des Begriffs „personenbezogener Daten“

- Auslegung des Begriffs ist umstritten:
  - Objektives Verständnis
  - Subjektives Verständnis
- EuGH, Urt. v. 19.10.2016 – C-582/14 – *Breyer*:

  Alle Mittel, die vernünftigerweise vom Verantwortlichen oder einem Dritten zur Bestimmung der betroffenen Person eingesetzt werden können sind zu berücksichtigen
- Direktive der Praxis: Im Zweifel ist von einem Personenbezug auszugehen

Anonyme und Pseudonyme Daten

Erwägungsgrund (26) DS-GVO

„[…] Einer **Pseudonymisierung** unterzogene personenbezogene Daten, die durch Heranziehung zusätzlicher Informationen einer natürlichen Person zugeordnet werden könnten, sollten als **Informationen über eine identifizierbare natürliche Person** betrachtet werden. […]

Die Grundsätze des Datenschutzes sollten daher **nicht für anonyme Informationen** gelten, d.h. für Informationen, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann.“

Anonyme und Pseudonyme Daten

- Pseudonymisierte Informationen
  - DS-GVO ist anwendbar
- Anonymisierte Informationen
  - DS-GVO **nicht** anwendbar
- Speicherung anonymisierter Daten in der Blockchain unterfällt nicht den Regelungen der DS-GVO

Personenbezogene Daten in private Blockchains

- Public Key in Transactions
  - jedenfalls Offenlegung der Identität gegenüber zentraler Stelle
  - Ggf. Ansprüche auf Auskunft gegen zentrale Stelle
  - Personenbezogenes Datum (+)
- Inhalt der Transaction
  - Hashwerte
  - Verschlüsselung
  - Personenbezogene Daten (+)

Datenverarbeitungen in der Industrie 4.0

- Blockchain & Industrie 4.0: Verarbeitung unternehmensbezogener Daten
  - (Ir-)Relevanz des Datenschutzrechts?

Erwägungsgrund (14) S. 2 DS-GVO

„Diese Verordnung gilt nicht für die Verarbeitung personenbezogener Daten juristischer Personen und insbesondere als juristische Person gegründeter Unternehmen, einschließlich Name, Rechtsform oder Kontaktdaten der juristischen Person."

Datenverarbeitungen in der Industrie 4.0

- Personenbezug und juristische Personen
  - Grundsätzlich (-)
  - EuGH, Urt. v. 9. 11. 2010 - C-92, 93/09 Rn. 53 – *Schecke*:
    Name bzw. die Firmierung der juristischen Person bestimmt die natürliche Personen
  - EuGH, Urt. v. 9.3.2017 – C-398/15 Rn. 34 – *Manni*:
    Angaben zu natürlichen Personen, die aufgrund ihrer Funktion als Organ einer Gesellschaft in ein Register eingetragen werden
  - EuGH, Urt. v. 10.12.2020 – C-620/19 Rn. 41 – *NRW/D.-H. T.*

    „Wie aus Art. 1 Abs. 1 der DSGVO hervorgeht, enthält diese Verordnung jedoch Bestimmungen zum Schutz personenbezogener Daten natürlicher Personen und erfasst nicht die Daten, die juristische Personen betreffen.“

RECHT-TESTBED

Datenschutzrechtliche Verantwortlichkeit

RECHT-TESTBED

Verantwortlichkeitskonzepte der DS-GVO

- Ausgangspunkt: Verantwortlicher und Auftragsverarbeiter als Regelungsadressaten des Datenschutzrechts
- Normative Konzepte
  - Alleinverantwortlichkeit, Art. 24 DS-GVO
  - Gemeinsame Verantwortlichkeit, Art. 26 DS-GVO
  - Auftragsverarbeitung, Art. 28 DS-GVO

Verantwortlichkeitskonzepte der DS-GVO

- Regulatorischer Ausgangspunkt: Zentrale Netzwerkstrukturen
- Herausforderungen im Kontext der Blockchain Technologie:
  - Dezentralität
  - Verschiedene Konzeptionsformen von Blockchain-Netzwerken
  - Reichweite der gemeinsamen Verantwortlichkeit

Voraussetzungen datenschutzrechtlicher Verantwortlichkeit

Art. 4 Nr. 7 DS-GVO

„‘Verantwortlicher‘ [ist] die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen **über die Zwecke und Mittel der Verarbeitung** von personenbezogenen Daten **entscheidet** […]“

RECHT-TESTBED

Voraussetzungen datenschutzrechtlicher Verantwortlichkeit

- „Entscheidungstrias“ des EuGH zur gemeinsamen Verantwortlichkeit
  1. EuGH, Urt. v. 5.6.2018, C-210/16 – *ULD/Wirtschaftsakademie SH*
     - Facebook und Fanpage-Betreiber = gemeinsame Verantwortliche
     - Fanpage-Betreiber beeinflusst Nutzungsstatistiken
  2. EuGH, Urt. v. 10.7.2018, C-25/17 - *Jehovan todistajat*
     - Religionsgemeinschaft und ihre verkündenden Mitglieder = gemeinsame Verantwortliche
     - Religionsgemeinschaft organisiert, koordiniert und motiviert zur Verarbeitung
  3. EuGH, Urt. v. 29.7.2019, C-40/17 – *Fashion ID*
     - Facebook und Webseitenbetreiber, der ein social plugin (Like-Button) eingebunden hat = gemeinsame Verantwortliche
     - Webseitenbetreiber profitiert bei ökonomischer Betrachtung durch bessere Listung

Verantwortlichkeit in privaten Blockchain-Netzwerken

- Verantwortlichkeit der zentralen Stelle bei Verarbeitungen im Rahmen der Zulassung zum Netzwerk

- Datenverarbeitungen im Netzwerk
  - Kriterien zur Allokation der Verantwortlichkeit
    - Kontrolle und Einfluss der zentralen Stelle
      - Steuerungsmöglichkeiten
      - Eingriffsmöglichkeiten
    - Inhaltlicher Entscheidungsspielraum der Teilnehmer

Verantwortlichkeit in privaten Blockchain-Netzwerken

- **Szenario 1: Zentrale Stelle bestimmt Zweck**
  - Alleinverantwortlichkeit der zentralen Stelle
  - Netzwerkteilnehmer als Auftragsverarbeiter

- **Szenario 2: Zentrale Stelle stellt lediglich eine technische Plattform bereit (str.)**
  - Alleinverantwortlichkeit der Teilnehmer
  - Gemeinsame Verantwortlichkeit aller Netzwerkteilnehmer
  - Gemeinsame Verantwortlichkeit Netzwerkteilnehmer + zentrale Stelle

Verantwortlichkeit in privaten Blockchain-Netzwerken

- **Szenario 2: Zentrale Stelle stellt lediglich Plattform für die Teilnehmer bereit (str.)**
- Netzwerkteilnehmer als Verantwortlicher?
  - Grad des Einflusses auf einzelne Transaktionen
  - Ggf. Eingriffsbefugnisse der zentralen Stelle

- Gemeinsame Verantwortlichkeit aller Netzwerkteilnehmer?
  - Regelmäßig kein Einfluss auf den Inhalt der Transaktionen anderer Netzwerkteilnehmer

- Gemeinsame Verantwortlichkeit zentrale Stelle + Teilnehmer?
  - EuGH, Urt. v. 10.7.2018, C-25/17 - *Jehovan todistajat*
    Gemeinsame Verantwortlichkeit aufgrund der Organisation und Koordination von Verarbeitungen
  - EuGH, Urt. v. 29.7.2019, C-40/17 – *Fashion ID*
    Gemeinsame Verantwortlichkeit aufgrund potenzieller ökonomischer Vorteile
  - Rolle der Entscheidungen in der Industrie 4.0 noch unklar

Verantwortlichkeit in privaten Blockchain-Netzwerken

- Allokation datenschutzrechtlicher Verantwortlichkeit hängt von der Organisation des Blockchain-Netzwerks im Einzelfall ab
- Ermittlung des Einflusses der zentralen Stelle auf die Verarbeitungen sowie der Rahmenbedingungen der Teilnahme am Netzwerk
- Bedeutung der gemeinsamen Verantwortlichkeit im Kontext privater Blockchain-Netzwerke weitgehend unklar

Legitimation der Datenverarbeitung

RECHT-TESTBED

Die Erlaubnistatbestände des Art. 6 Abs. 1 DS-GVO

Art. 6 Abs. 1 DS-GVO

„Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:

a) Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;

b) die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen;

c) die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt;

d) die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen;

e) die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;

f) die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

Unterabsatz 1 Buchstabe f gilt nicht für die von Behörden in Erfüllung ihrer Aufgaben vorgenommene Verarbeitung.“

Legitimation von Datenverarbeitungen in der Blockchain

- Vorfrage: Binnenverhältnis der Erlaubnistatbestände des Art. 6 Abs. 1 DS-GVO
  - e.A. Primat der Einwilligung
  - a.A. (Faktische) Subsidiarität der Einwilligung
  - h.M. Gleichrang der Erlaubnistatbestände

Legitimation von Datenverarbeitungen in der Blockchain

- Einwilligung (Art. 6 Abs. 1 lit. a) DS-GVO)
  - e.A.: Kann in private Blockchains funktionieren
  - Erfordernis der aktiven Einwilligung
  - Betroffener kann die Einwilligung jederzeit widerrufen (Art. 7 Abs. 3 DS-GVO)
  - Kaum praktikabel, Betroffener mitunter unbekannt

- Zur Erfüllung eines Vertrages erforderliche Verarbeitungen (Art. 6 Abs. 1 lit. b) DS-GVO)
  - Reichweite des Erlaubnistatbestandes ist umstritten
  - Im Grundsatz aber potenziell anwendbarer Erlaubnistatbestand

Legitimation von Datenverarbeitungen in der Blockchain

- Zur Erfüllung rechtlicher Verpflichtungen erforderliche Verarbeitungen (Art. 6 Abs. 1 lit. c) DS-GVO)
  - Etwa bei Bestehen von Dokumentationspflichten

- Zur Wahrung berechtigter Interessen erforderliche Verarbeitungen (Art. 6 Abs. 1 lit. f) DS-GVO)
  - Rechtsverteidigung
  - Interesse an Rechtssicherheit durch Dokumentation
  - Interesse an der Validierung von Informationen in der Blockchain
  - Differenzierung danach ob Betroffener an der Transaktion beteiligt ist

Blockchain & Betroffenenrechte

RECHT-TESTBED

Die Rechte des Betroffenen unter Geltung der DS-GVO

- Betroffenenrechte (Art. 12 ff. DS-GVO)
  - Informationspflichten (Art. 13 f. DS-GVO)
  - Auskunftsrecht (Art. 15 DS-GVO)
  - Recht auf Berichtigung (Art. 16 DS-GVO)
  - Recht auf Löschung (Art. 17 DS-GVO)
  - Recht auf Einschränkung der Verarbeitung (Art. 18 DS-GVO)

- Spannungsfeld: Berichtigungs-/Löschungsanspruch **vs.** Unveränderlichkeit
- Befunde in der Literatur: „Betroffenenrechte laufen ins Leere“ oder deren Umsetzung sei „nahezu unmöglich“

Betroffenenrechte in der Blockchain

- Rechtliche Ansätze:
  - Teleologische Reduktion des Begriffs der „Berichtigung“
  - Ausschluss des Löschungsanspruchs gem. Art. 17 Abs. 3 DS-GVO i.V.m. § 239 HGB analog
  - Primärrechtsinduzierte restriktive Auslegung des Löschungsanspruchs aus Art. 17 Abs. 1 DS-GVO
  - Beschränkung des Löschungsanspruchs bei pseudonymisierten Daten *de lege ferenda*

Betroffenenrechte in der Blockchain

- Technische Ansätze
  - Nachträgliche Veränderung verketteter Blöcke durch kryptographische Verfahren („*rewritable Blockchain*“)
  - Referenzierung *off-chain* gespeicherter personenbezogener Daten
  - Verschlüsselte Speicherung *on-chain* und Löschen des *off-chain* gespeicherten Entschlüsselungskeys
  - *Pruning*: Löschung von Informationen aus „älteren“ Blöcken der Blockchain

Fazit

Fazit

- Die Verarbeitung personenbezogener Daten in private Blockchain unterfällt der DS-GVO.
- Die umstrittene Auslegung der Vorschriften der DS-GVO birgt Rechtsunsicherheiten.
- Die „Intermediatisierung“ bei private Blockchains wirft Fragen bei der Allokation datenschutzrechtlicher Verantwortlichkeit auf.
- Der datenschutzkonforme Einsatz von Blockchain-Technologien hängt von der technischen Ausgestaltung im Einzelfall ab.

Vielen Dank!
Fragen?

jonas.baumann@uni-saarland.de

https://legaltestbed.org

RECHT-TESTBED