Blockchain und Datenschutz

Ursula Sury

Um was geht es?

Grundprinzip der Blockchain ist ein auf **mehreren Rechnern** identisch vorhandenes und grundsätzlich offenes **Register** von **Informationen**.
Diese Informationen können sich auf eine natürliche **Person** beziehen und dann stellen sich die Fragen des **Datenschutzes**.

Zulässigkeit und Zweck der Blockchain

Als erstes stellt sich die Frage, warum es zulässig ist, diese Information überhaupt und zu welchem Zweck in die Blockchain zu stellen.
Die Blockchain wird zu einem **bestimmten** gesetzlichen oder vertraglichen **Zweck** geführt. Fehlt eine gesetzliche Grundlage, so muss aus Datenschutzsicht unbedingt eine **Einwilligung** der betroffenen **Person** vorliegen.
Was die Anforderung an die Einwilligung anbelangt, so ist es wichtig, dass der betroffenen Person genau **bewusst** ist, welche Dimensionen von **Bearbeitungen** vorgenommen werden, insbesondere auch, wer **Zugriff** hat, was mit den Infos durch **wen** gemacht wird, wie lange es wo aufbewahrt wird etc. Es sind klare **Informationen** über den gesamten LifeCycle der Daten zu **geben**.
Informationen, die in der Blockchain sind, sind als solche **nicht** mehr **veränderbar**. Jede Änderung ist nur über Ergänzung in der Blockchain möglich. Aus diesem Grund ist auch ein Löschen von Information im Sinne eines (absoluten) Rechtes auf **Vergessen** wie es in der EU-DSGVO statuiert ist **nicht möglich**.
Betroffene Personen haben Anspruch auf **Richtigkeit** der sie betreffenden Informationen. Dies wird durch die Blockchain sowohl unterstützt als auch erschwert, indem eben Korrekturen nur durch nachvollziehbare Veränderungen möglich sind.

Formen der Blockchain

Da die Blockchain über verteilte ledger/Verzeichnisse auf verschiedenen miteinander verbundenen Rechnern (peer 2 peer) funktioniert, impliziert ein **Aufnehmen** von **Personendaten** in die Blockchain immer auch ein mehr oder weniger breites **Veröffentlichen** und damit verbunden mehr oder weniger **Zugriffe**. Mit dem Veröffentlichen von Personendaten werden diese einem breiten Personenkreis zugänglich gemacht. Hier stellt sich die Frage, welche Art von Blockchain eingesetzt wird, private, halbprivate, öffentliche oder Konsortiumsblockchain.

- **Private Blockchains** (private blockchains/ private permissioned blockchains)[1]: Die private Blockchain wird von einer einzelnen Organisation kontrolliert und ist somit zentralisiert. Die Organisation bestimmt wer Informationen lesen kann, wer Transaktionen übermitteln kann, etc. Einsatzmöglichkeiten sind z. Bsp. Entwicklungs- und Testumgebeungen.

- **Halbprivate Blockchains** (private blockchains/ private permissioned blockchains): Ein Einzelnes Unternehmen betreibt die Blockchain. Zugriffsrechte werden anhand von Kriterien abgegeben. Die halbprivate Blockchain kann gut für Business-to-Business oder Behörden eingesetzt werden.

- **Öffentliche Blockchains** (public blockchains/ public permissionless blockchain): Jeder kann in der öffentlichen Blockchain Informationen Lesen und Transaktionen tätigen. Jede Transaktion ist öffentlich, die Teilnehmer bleiben aber anonym. Öffentliche Blockchains sind z. Bsp. diverse Kryptowährungen (Bitcoin und Ethereum).

- **Konsortiumblockchains** (federated blockchains/ je nachdem ob die Transaktionen öffentlich gelesen werden oder nicht, public permissioned blockchain oder private permissoned blockchain): Eine ausgewählte Gruppe kontrolliert die Blockchain. Das Recht die Transaktionen zu lesen, kann jedem oder nur den Teilnehmenden gewährt werden. Anwendungen könnten sich z. Bsp. bei einer Gruppe von Finanzinstituten oder andere Unternehmen finden lassen.

Zentral verwaltete Blockchains sind gegen aussen abgeschottet, deren Teilnehmer sind bekannt. Es können datenschutzrechtliche Mitteilungen

[1] Die Begriffe sind noch nicht einheitlich definiert.

getätigt und Einwilligungen etc. eingeholt werden. Sie können **datenschutzkonform** betrieben werden. Zu den zentral verwalteten Blockchains gehören **private/ halbprivate Blockchains** je nach Aufbau könnte dies auch eine **Konsortiumblockchain** erfüllen. Bei **dezentral verwalteten** Blockchains sind die datenschutzrechtlichen Anforderungen **kaum einzuhalten**, da es keinen rechtlichen Verantwortlichen gibt, wie es z.B. eine EU-DSGVO vorschreibt. Dazu gehört vor allem die **öffentliche Blockchain**, je nach Ausgestaltung aber auch die **Konsortiumblockchain**.

Blockchain hinterlässt Fragen

Da Blockchain sich technologisch **kaum auf** das Gebiet der **Schweiz beschränken** wird und/oder kaum nur Informationen von Schweizer Bürgern sich dort halten werden, stellt sich die Frage, welches Recht für Datenschutzfragen anwendbar ist. Damit verknüpft ist die Frage, **wer** denn für die Blockchain **verantwortlich** ist und somit eingeklagt werden kann. An dieser Frage wird sich dann auch mitorientieren, wo der Gerichtsstand für allfällige Klagen sein könnte. Aus der Kumulierung dieser Fragen lässt sich unschwer folgern, dass eine **Vollstreckung** von **Datenschutzansprüchen** sowohl durch eine betroffene Person als auch durch eine Datenschutzaufsichtsstelle (wie z.B. der eidgenössische Datenschutz und Öffentlichkeitsbeauftragter) im Bereich Blockchain **sehr schwierig** sein wird.

Eine andere Frage, die im Umgang mit Blockchain diskutiert wird ist, ob man über **Anonymisierung** den Personenbezug und somit die Anwendbarkeit des **Datenschutzes eliminieren** könnte. Da Anonymisierung in technischer Hinsicht äusserst anspruchsvoll ist und deshalb mit einem gewissen Aufwand eine Zuordnung der Daten wieder möglich wird, ist dies sehr **schwierig umzusetzen**.

Automatisierte Einzelentscheide

Wenn Personendaten **automatisiert**, d.h. ohne menschliche Überprüfung **bearbeitet** werden und sich daraus (negative) **Folgen** für die betroffene Person ergeben, hat diese das Recht, dazu **Stellung** zu **nehmen**. Das

heisst der **Datenbearbeiter** muss die betroffene Person in irgendeiner Art **kontaktieren** und mit der dann eingegangenen Stellungnahme etwas machen.

Smarte Contracts

Smarte Contracts dienen dazu, **automatisiert Verträge** zu **erfüllen** (nicht Verträge abzuschliessen, vgl. dazu Artikel im Informatikspektrum zu Smarte Contracts). Auch für das Ausführen von automatisierten Einzelentscheiden wären Smarte Contracts prädestiniert.
Hier stellt sich wieder die Frage, **wie** bei einer relativ anonymen Blockchain denn die **Information** und die **Sicherung** der **Rechte** der **Betroffenen** tatsächlich von wem **umgesetzt** würde.

Zusammenfassung

- Nicht jede Form von **Blockchain** erfüllt den Datenschutz, bzw. es ist schwierig mit einer Blockchain den nötigen Datenschutzstandard zu erreichen. Folgende Punkte sind zu beachten.
    - **Einwilligung** der betroffenen Person, Tragweite muss erkannt werden, es muss genügend informiert werden.
    - Personendaten müssen **korrekt** sein. **Anpassung** nicht immer einfach, da Änderungen nur Ergänzungen sind.
- Noch ungelöste **Fragestellungen** sind u.a. welches Recht angewendet wird oder wer, vor allem bei offenen Systemen, der Verantwortliche ist.
- **Smarte Contracts** dienen dazu **automatisierte Einzelentscheidungen** zu erfüllen.

Ursula Sury ist selbständige Rechtsanwältin in Luzern, Zug und Zürich (CH) und Vizedirektorin an der Hochschule Luzern - Informatik. Sie ist zudem Dozentin für Informatikrecht, Datenschutzrecht und Digitalisierungsrecht.