Ausgewählte datenschutzrechtliche Fragen im Zusammenhang mit der Personenzertifizierung in der Blockchain

Gutachten

vorgelegt von

Mag. iur. Dr. iur. Nikolaus Forgó

Universitätsprofessor an der Universität Wien

Mag. iur. Žiga Škorjanc

Universitätsassistent an der Universität Wien

am

21.12.2018

Inhaltsverzeichnis

1. Sachverhalt und Auftrag

Die Auftraggeberin dieser Stellungnahme ist die Wirtschaftskammer Österreich, Wiedner Hauptstraße 63, A-1045 Wien („**WKÖ**"). Als die B2B-Standardisierungsplattform innerhalb der WKÖ fungiert die AUSTRIAPRO, Verein zur Förderung der elektronischen Datenübermittlung im Geschäftsverkehr, ein Verein nach dem Vereinsgesetz 2002 mit Vereinssitz in Wien, in das Vereinsregister zu Vereinsregisterzahl ZVR-ZI 205085897 eingetragen („**AUSTRIAPRO**").[1] Die AUSTRIAPRO hat Arbeitskreise eingerichtet, die als Plattformen des Informationsaustausches und der Diskussion aktueller E-Business Themen dienen.[2]

Unter anderem wurde der Arbeitskreis Blockchain eingerichtet, welcher sich mit Anwendungen, Nutzen und Risiken der Blockchain Technologie in verschiedenen Wirtschaftsbereichen befasst. Die Arbeitsgruppe Zertifizierungen des Arbeitskreises hat einen Pilotprojekt über „Zertifizierung in der Blockchain" mit dem Arbeitstitel „CertiChain" gestartet.[3] Im Rahmen des Projektes wird ein technischer Pilot ausgearbeitet, mit dem klassische Personen-Zertifizierungen (von TÜV, Quality Austria…) nach EN ISO/IEC 17024 *„Konformitätsbewertung-Allgemeine Anforderungen an Stellen, die Personen zertifizieren"*, Ausgabe: 2012-10-15, in einer Blockchain abgebildet und beauskunftet werden sollen („**Pilotprojekt**").

Unter Personen-Zertifizierungen werden die Zertifizierungen von Personen im Produktions- und Dienstleistungssektor, wie etwa Kunststoffschweißer/in nach ÖNORM EN 13067, Process Manager/in (PcM) oder Qualitätsassistent/in (QAss), verstanden.[4] Personenzertifikate werden in Österreich derzeit von 14 akkreditierten Zertifizierungsstellen für Personen ausgestellt.[5]

Bisher sind Personenzertifikate weder durchgängig digitalisiert noch in einer zentralen Datenbank zusammengefasst bzw. vernetzt, was die **Beauskunftung** (Suche und Validierung) aufwändig macht. Dies war zugleich der **Anlass für das Pilotprojekt**.

Begleitend zur technischen und organisatorischen Umsetzung bzw. Weiterentwicklung des Pilotprojekts wurde das gegenständliche Rechtsgutachten erstellt, das auf die ausgewählten datenschutzrechtlichen Fragen im Zusammenhang mit der Abbildung und Beauskunftung von Personenzertifikaten in der Blockchain im Rahmen des Pilotprojekts eingeht.

---

[1] Vgl. https://www.wko.at/service/netzwerke/austriapro-ueber-austriapro.html.
[2] Vgl. https://www.wko.at/service/netzwerke/austriapro-arbeitskreise.html.
[3] Dieses Projekt wurde uns anhand der Präsentation Update: Zertifizierungen in der Blockchain, Status September 2018, vorgestellt.
[4] Für weitere Beispiele siehe etwa *Zertifizierungsstelle der WIFI Österreich*, Zertifizierte Kompetenz, http://zertifizierung.wifi.at/uploads/WIFI_SCH%C3%9620_Zertifizierte_Kompetenz_Folder_A4_4s.pdf.
[5] Vgl. *BMDW*, Akkreditierte Zertifizierungsstellen für Personen, gemäß EN ISO/IEC 17024:2012, https://www.bmdw.gv.at/TechnikUndVermessung/Akkreditierung/Documents/certification%20bodies%20for%20persons.pdf.

2. Fragestellung

Im Rahmen des gegenständlichen Gutachtens wird untersucht, **unter welchen Bedingungen die Zertifikate, die von Zertifizierungsstellen für Personen nach EN ISO/IEC 17024 *„Konformitätsbewertung-Allgemeine Anforderungen an Stellen, die Personen zertifizieren“*, Ausgabe: 2012-10-15, ausgegeben werden, in einem Blockchain-System gespeichert werden dürfen**.

Um die Aufnahme von Echtdaten über zertifizierte Personen in die Blockchain zu ermöglichen, ist auf die Ausgestaltung des im Rahmen des Pilotprojekts entwickelten Blockchain-Systems, insbesondere im Hinblick auf die Zulässigkeit der Verarbeitung personenbezogener Daten, einzugehen. Es werden unter anderem folgende Aspekte untersucht:

a) Wie wird das Zertifizierungswesen, inklusive Beauskunftung, geregelt und wie diese Normen die datenschutzrechtliche Zulässigkeit der Personenzertifizierung in einer Blockchain beeinflussen.

b) Welche personenbezogenen Daten dürfen bei der Personenzertifizierung in einem Blockchain-System in der Blockchain selbst (*on chain*) gespeichert werden?

c) Welche Teilnehmer wird es in der zentralen Datenbank für Personenzertifikate geben, welche Rollen werden sie im Blockchain-System haben und wie diese datenschutzrechtlich einzuordnen sind?

d) Auf welcher datenschutzrechtlicher Rechtsgrundlage können in der zentralen Datenbank für Personenzertifikate personenbezogene Daten verarbeitet werden?

e) Welche sonstigen Maßnahmen können die datenschutzkonforme Verarbeitung von personenbezogenen (Zertifikats-)Daten in der zentralen Datenbank für Personenzertifikate, insbesondere im Hinblick auf die Erfüllung der Rechte der betroffenen Personen, möglich machen?

f) Könnte eine ausdrückliche Anordnung etwa durch eine Verordnung einer Verwaltungsbehörde oder Leitfäden der Akkreditierung Austria die aktuelle Rechtslage beeinflussen?

3. Zusammenfassung der Ergebnisse

a) Die wesentliche Rechtsgrundlage der Personenzertifizierung ist die Zertifizierungsnorm EN ISO/IEC 17024 *„Konformitätsbewertung-Allgemeine Anforderungen an Stellen, die Personen zertifizieren“*, Ausgabe: 2012-10-15 (im Folgenden „**ISO 17024**“). Die ISO 17024 verpflichtet die Zertifizierungsstellen die Informationen über aktuelle und gültige Personenzertifikate öffentlich zur Verfügung zu stellen, welche (zumindest) den – ebenfalls in ISO 17024 geregelten – Mindestinhalt eines Personenzertifikats umfassen. Die Zertifizierungsstellen sind nach ISO 17024 hingegen nicht verpflichtet, über nicht mehr gültige Personenzertifikate Auskunft zu geben (vgl. Punkt 4.a)).

b) In der Blockchain selbst (*on chain*) sollen die Zertifikatsdaten gespeichert werden, welche in der Regel personenbezogene Daten darstellen (vgl. Punkt Punkt 4.b)i)). Die Verarbeitung von personenbezogenen Daten in der zentralen Datenbank für Personenzertifikate wird zum Zwecke der Erteilung von Auskünften über Personenzertifikate an die Öffentlichkeit entsprechend der Anforderungen an öffentliche Informationen gemäß ISO 17024 erfolgen (vgl. Punkt 4.c)i)), daher ist sie auf die personenbezogenen Daten zu beschränken, die zur Beauskunftung der Personenzertifikate oder zum Betrieb bzw. zur Funktionsfähigkeit der zentralen Datenbank für Personenzertifikate erforderlich sind (vgl. Punkt 4.c)v)).

   Zu einer der ISO 17024 entsprechenden Beauskunftung der Personenzertifikate sind (zumindest) die Angaben über aktuelle und gültige Personenzertifikate im Umfang des Mindestinhalts eines Personenzertifikats erforderlich. Diese dürfen in der Blockchain gespeichert werden (vgl. Punkt 4.a)ii)(1), Punkt 4.b)i) und Punkt 4.c)iv)).

   Hingegen verlangt die ISO 17024 nicht die Beauskunftung von abgelaufenen Zertifikaten. Da diesbezüglich keine Informationspflicht (mehr) besteht, ist die Beauskunftung, der in diesen Zertifikaten enthaltenen personenbezogenen Daten, nach dem Grundsatz der Datenminimierung zu unterlassen (vgl. Punkt 4.c)v)).

c) Die Teilnehmer des Blockchain-Systems werden unterschiedliche Rollen haben, was auch zu unterschiedlichen Berechtigungen und Zugriffsmöglichkeiten, voraussichtlich über eine Web-Oberfläche, führen wird. Zwar sollte jeder Teilnehmer einen Blockchain-Knoten (*Node*) betreiben, allerdings wird nur gewissen Teilnehmern, die Möglichkeit zukommen, in die Blockchain zu schreiben (*„schreibende Teilnehmer“*). Diese sind als datenschutzrechtliche Verantwortliche der zentralen Datenbank zu qualifizieren. Voraussichtlich wird es sich dabei um die Akkreditierung Austria und die Zertifizierungsstellen für Personen handeln (vgl. Punkt 4.d)i)). Die nicht-schreibenden Teilnehmern, die „einfache“ Betreiber von Blockchain-Knoten sind, sind als Auftragsverarbeiter zu qualifizieren.

Im Lichte des Datenminimierungsgrundsatzes und wegen der praktischen Durchsetzbarkeit der datenschutzrechtlichen Vorgaben ist zweckmäßig, die Anzahl der nichtschreibenden Teilnehmer zu beschränken. Dies kann erfolgen, indem die Blockchain öffentlich einsehbar wird oder Serviceanbieter als Auskunftsstellen für die Öffentlichkeit und somit eine Art „Gatekeeper" des Blockchain-Systems eingesetzt werden. Im letzten Fall wären Serviceanbieter „einfache" Betreiber von Blockchain-Knoten und damit Auftragsverarbeiter. Hingegen wären die interesseierten Unternehmen und Personen, welche die Auskünfte über Zertifikate erhalten, in beiden Fällen nicht Teilnehmer des Blockchain-Systems, sondern als Empfänger der personenbezogenen Daten und als Dritte zu qualifizieren (vgl. Punkt 4.c)iii) und Punkt 4.d)ii)).

Beim geplanten Blockchain-System handelt es sich um eine zulassungsbeschränkte Blockchain. Die Definition der Rollen der Teilnehmer, insbesondere Berechtigungen, Zugriffsmöglichkeiten und Zulassung zum Blockchain-System, und die Zuteilung der beschriebenen Rollen sowie die Beziehungen und Kooperation zwischen den Teilnehmern können entweder durch eine zu schaffende allgemeine Rechtsgrundlage, wie etwa eine Verordnung, oder alternativ durch eine Vereinbarung zwischen den Teilnehmern des Blockchain-Systems erfolgen (vgl. Punkt 4.c)ii)).

d) Die Verarbeitung von personenbezogenen Daten im Rahmen des Betriebs der zentralen Datenbank für Personenzertifikate ist rechtmäßig, wenn *„mindestens"* ein gesetzlicher Erlaubnistatbestand erfüllt ist oder die betroffene Person eingewilligt hat.

   Eine Datenverarbeitung ist unter anderem rechtmäßig, wenn sie zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist, der der Verantwortliche unterliegt. Die Rechtsgrundlage für die Verarbeitung personenbezogener Daten, die zur Beauskunftung der Personenzertifikate oder zum Betrieb bzw. zur Funktionsfähigkeit der Datenbank erforderlich sind, ist die ISO 17024, welche die Zertifizierungsstellen zur Erteilung von Informationen an interesseierte Unternehmen und Personen verpflichtet. Zusätzlich kann diese Datenverarbeitung auf ein berechtigtes Interesse der Verantwortlichen und der interesseierten Unternehmen und Personen gestützt werden.

e) Die Blockchain-Systeme stehen wegen der „Unveränderbarkeit" der in der Blockchain gespeicherten Daten in einem Spannungsverhältnis mit der effektiven Erfüllung bestimmter Rechte der betroffenen Personen, die die Veränderung oder die Löschung eines in der Blockchain gespeicherten Datums voraussetzen (vgl. Punkt 4.f)).

   Das Recht auf Berichtigung kann in der Blockchain durch sog. „Reverse transactions" als ergänzende Erklärungen erfüllt werden. Der neue Block mit inhaltlich richtigen personenbezogenen Daten berichtigt den alten Block mit unrichtigen Daten und wird anstatt diesen beauskunftet. Der alte Block ist anschließend grundsätzlich zu löschen (vgl. Punkt 4.f)ii)(1)).

Der Begriff der Löschung umfasst jedwede Art der Unkenntlichmachung, nicht nur physische Vernichtung. Wesentlich ist, dass die Daten für den Verantwortlichen unlesbar geworden sind oder diesem nicht mehr zur Verfügung stehen (vgl. Punkt 4.f)iv)(1)(b)). Eine technische Implementierung des Rechts auf Löschung in der Blockchain ist – aus Perspektive des Datenschutzrechts – möglich. Bei (zulassungsbeschränkten) Blockchain-Systemen sind mehrere technische und organisatorische Verfahren, wie vor allem Puning und Chameleon Hash, welche eine Änderung der in der Blockchain gespeicherten Daten (*on chain*) ermöglichen, denkbar. Die angewendeten Verfahren müssen im Einzelfall mit der wirkungsorientierten Löschung iSd DSGVO äquivalent sein (vgl. Punkt 4.f)iv)(1)(c)4.f)iv)(1)(d)). Ist in einem Blockchain-System die Löschung der personenbezogenen Daten (technisch) nicht – oder nur mit unverhältnismäßigen Aufwand – umsetzbar, kann die betroffene Person unseres Erachtens in Verfolgung ihrer Grundrechte und Grundfreiheiten und/oder sonstigen legitimen Interessen auf ihr Recht auf Löschung verzichten, soweit dies ein geeignetes und erforderliches Mittel zur Erreichung eines dieser Interessen ist und nach Abwägung des Nutzens für die betroffene Person und der Beeinträchtigung ihrer grundrechtlich geschützten Position angemessen ist. In diesem Fall ist die Verarbeitung von Daten, welche mangels Verzichts zu löschen wären, jedoch einzuschränken (vgl. Punkt 4.f)iv)(5)).

f) Die im gegenständlichen Gutachten dargestellte Rechtslage kann zudem durch objektives Recht gestaltet werden.[6] Zu diesem Zweck könnte eine rechtliche Verpflichtung der Zertifizierungsstellen für Personen und (möglicherweise) der Akkreditierung Austria zur Führung (bzw. zum Betrieb) einer zentralen Datenbank für Personenzertifikate aller Zertifizierungsstellen für Personen mit einem (nationalen) Gesetz oder mit einer Verordnung der Bundesministerin für Digitalisierung und Wirtschaftsstandort vorgesehen werden (vgl. Punkt 4.e)i)). Hingegen kommt den Leitfäden der Akkreditierung Austria (wohl) nicht die erforderliche Rechtsqualität und Rechtsbindungswirkung zu, um sie als Rechtsvorschrift des Mitgliedstaats Österreich im Sinne der DSGVO qualifizieren zu können (vgl. Punkt 4.d)i)).

   Durch ein Gesetz oder eine (Register-)Verordnung kann zunächst die Rechtsgrundlage für die Verarbeitung von personenbezogenen (Zertifikats-)Daten in der zentralen Datenbank für Personenzertifikate geschaffen werden (vgl. Punkt 4.e)i)). Ferner können nicht nur die Rollen der Teilnehmer, insbesondere Berechtigungen, Zugriffsmöglichkeiten und Zulassung zum Blockchain-System, im Blockchain-System definiert und zugeteilt werden (vgl. Punkt 4.c)ii)), sondern auch die Beziehungen zwischen den gemeinsam Verantwortlichen (vgl. Punkt 4.d)i)) sowie zwischen den Verantwortlichen und den Auftragsverarbeitern (vgl. Punkt 4.d)ii)), insbesondere hinsichtlich der Erfüllung der Rechte der betroffenen Personen (vgl. Punkt 4.f)iv)(1)(d)), geregelt werden.

[6] An dieser Stelle werden die Möglichkeiten, die an der jeweiligen Stelle im Gutachten aufgezeigt werden, zusammengefasst und mit entsprechenden Verweisen versehen.

Zudem kann eine (allfällige) Beschränkung der Rechte der betroffenen Personen vorgesehen werden (vgl. Punkt 4.f)iv)(4) und Punkt 4.f)v)). Die vorgesehene Beschränkung muss den Wesensgehalt der Grundrechte und Grundfreiheiten achten sowie in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme darstellen. Des Weiteren hat die die Beschränkung enthaltende Rechtsvorschrift gewisse inhaltliche Mindestanforderungen zu erfüllen und etwa den Umfang der vorgenommenen Beschränkungen vorzusehen. Werden die Rechte der betroffenen Personen, insbesondere das Recht auf Löschung, (entsprechend) beschränkt, ist kein Verzicht der jeweiligen betroffenen Person erforderlich (vgl. Punkt 4.f)v)).

4. Rechtliche Würdigung

a) Rechtliche Grundlagen der Personen-Zertifizierung

Im Europäischen Binnenmarkt besteht ein System der **Konformitätsbewertungen**, welches diverse anerkannte Prüfungen, Kalibrierungen und Zertifikate umfasst, die Sicherheit geben, dass die in Verkehr gebrachten Produkte bzw. erbrachten Dienstleistungen den Harmonisierungsvorschriften der Europäischen Gemeinschaft entsprechen. Diese Konformitätsbewertungen werden von Konformitätsbewertungsstellen ausgestellt, die ihrerseits durch eine nationale Akkreditierungsstelle akkreditiert werden müssen. Die Akkreditierung ist dabei als die formelle Anerkennung zu verstehen, dass eine Konformitätsbewertungsstelle die jeweils für sie geltenden Anforderungen an Qualifikation und Ausstattung erfüllt und sie damit als kompetent gilt.[7]

i) Rechtsgrundlagen

Die **gesetzliche Grundlage** für die Akkreditierung stellt die **Verordnung (EG) Nr. 765/2008** des Parlamentes und des Rates vom 9. Juli 2008 über die Vorschriften für die Akkreditierung und Marktüberwachung im Zusammenhang mit der Vermarktung von Produkten und zur Aufhebung der Verordnung (EWG) Nr. 339/93 des Rates dar. In Ergänzung dieser EU-Verordnung regeln das Akkreditierungsgesetz 2012 BGBl. I Nr. 28/2012 („**AkkG**“) und die Verordnungen auf dessen Basis[8] die Akkreditierung von Konformitätsbewertungsstellen (insbesondere Prüf-, Inspektions-, Kalibrier- und Zertifizierungsstellen) und legen die erforderlichen Verfahrensbestimmungen fest (§ 2).[9] Die österreichische Akkreditierungsstelle ist die Bundesministerin für Digitalisierung und Wirtschaftsstandort. Sie hat die Akkreditierung Austria, eine Organisationseinheit innerhalb ihres Wirkungsbereiches, mit dieser Aufgabe betraut (§ 3). Diese hat 14 **Zertifizierungsstellen für Personen** als Konformitätsbewertungsstellen für Personen-Zertifizierung akkreditiert.[10]

Bei der Akkreditierung von Konformitätsbewertungsstellen, die Personen zertifizieren, sind neben gesetzlichen Grundlagen noch die ***„normative Grundlagen“***, nämlich EN ISO/IEC 17024 *„Konformitätsbewertung-Allgemeine Anforderungen an Stellen, die Personen zertifizieren“*,

---

[7] Vgl. dazu https://www.bmdw.gv.at/TechnikUndVermessung/Akkreditierung/Seiten/default.aspx.

[8] Akkreditierungsgebührenverordnung, BGBl. Nr. 70/1994 idgF, Akkreditierungsversicherungsverordnung, BGBl. II Nr. 13/1997 idgF und Akkreditierungszeichenverordnung, BGBl. II Nr. 116/2013 idgF.

[9] Vgl. *Akkreditierung Austria*, Leitfaden L05_Akkreditierungserfordernisse für Konformitätsbewertungsstellen_V07_20170929, Punkt 1.1, https://www.bmdw.gv.at/TechnikUndVermessung/Akkreditierung/Documents/Leitfaden%20L05_Akkreditierungserfordernisse_V07_20170929.pdf.

[10] Die Akkreditierungsumfänge der Zertifizierungsstellen von Personen werden als Beilagen zu den Akkreditierungsbescheiden integrierender Bestandteil und sind aus folgendem Verzeichnis ersichtlich https://www.bmdw.gv.at/TechnikUndVermessung/Akkreditierung/Seiten/Akkreditierungsumfaenge.aspx; vgl. dazu auch https://www.bmdw.gv.at/TechnikUndVermessung/Akkreditierung/Seiten/AkkreditiertePIZ-Stellen.aspx.

Ausgabe: 2012-10-15 (im Folgenden „**ISO 17024**“), sowie *„weitere anwendbare Grundlagen für die Akkreditierung von Konformitätsbewertungsstellen“*, insbesondere die Leitfäden der Akkreditierung Austria, zu berücksichtigen.[11]

Die Bundesministerin für Digitalisierung und Wirtschaftsstandort *„kann mittels Verordnung die Fundstellen der Leitfäden der Akkreditierung Austria unter Bedachtnahme auf vergleichbare unionsrechtliche Vorschriften und Richtlinien internationaler Organisationen kundmachen und diese Leitfäden für verbindlich erklären, sofern dies zur Sicherung der Anerkennung der Konformitätsbewertungsstellen im Vergleich zum internationalen Niveau erforderlich ist oder dies eine zeit- und kostensparende Beurteilung der Anträge erleichtert“.*[12] Eine solche Verordnung wurde – soweit ersichtlich – hinsichtlich der zur Zeit veröffentlichen Leitfäden nicht erlassen.[13]

ii) EN ISO/IEC 17024 „Konformitätsbewertung-Allgemeine Anforderungen an Stellen, die Personen zertifizieren“

Die ISO 17024 wurde mit dem Ziel erarbeitet, eine weltweit anerkannte Vergleichbarkeit für Organisationen, die Personen zertifizieren, zu erreichen und zu fördern und das Umfeld für eine gegenseitige Anerkennung und den globalen Austausch von Personal zu bilden.[14] Sie enthält **Grundsätze und Anforderungen für eine Stelle, die Personen anhand spezifischer Anforderungen zertifiziert**, und schließt die Entwicklung und Aufrechterhaltung eines Zertifizierungsprogramms für Personen ein.[15] Das Zertifizierungsprogramm wird dabei als Kompetenz, im Sinne von Fähigkeit, Wissen und Fertigkeiten anzuwenden, um beabsichtigte Ergebnisse zu erzielen, und andere Anforderungen, bezogen auf Personengruppen mit spezifischen Tätigkeiten oder Fertigkeiten, definiert.[16]

Neben den allgemeinen Anforderungen wie Organisation als eine juristische Person oder ein festgelegter Teil davon (Punkt 4.1) und Handhabung der Unparteilichkeit (Punkt 4.3) regelt ISO 17024 folgende Regelungsgegenstände: Strukturelle Anforderungen (Punkt 5), Anforderungen an Ressourcen, insbesondere Personal (Punkt 6), **Anforderungen an Aufzeichnungen**

---

[11] *Akkreditierung Austria*, Leitfaden L05_Akkreditierungserfordernisse für Konformitätsbewertungsstellen_V07_20170929, Punkt 1.2 und 1.3, https://www.bmdw.gv.at/TechnikUndVermessung/Akkreditierung/Documents/Leitfaden%20L05_Akkreditierungserfordernisse_V07_20170929.pdf, **vgl. dazu auch** § 7 Abs 1 Z 1 AkkG iVm Mitteilung der Kommission im Rahmen der Durchführung der Verordnung (EG) Nr. 765/2008 des Europäischen Parlaments und des Rates, Beschluss Nr. 768/2008/EG des Europäischen Parlaments und des Rates, Verordnung (EG) Nr. 1221/2009 des Europäischen Parlaments und des Rates (2016/C 293/06), https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:52016XC0812(07) **und** Vorwort der ISO 17024: *„Diese Europäische Norm muss den Status einer nationalen Norm erhalten, entweder durch Veröffentlichung eines identischen Textes oder durch Anerkennung bis Januar 2013, und etwaige entgegenstehende nationale Normen müssen bis Januar 2013 zurückgezogen werden.“*

[12] § 7 Abs 2 AkkG.

[13] Vgl. Leitfäden für Konformitätsbewertungsstellen & Begutachter, https://www.bmdw.gv.at/TechnikUndVermessung/Akkreditierung/Seiten/DownloadsPIZ.aspx.

[14] ISO 17024, Einleitung.

[15] ISO 17024, Punkt 1.

[16] ISO 17024, Punkt 3.2 und 3.6.

und Informationen (Punkt 7), Zertifizierungsprogramme (Punkt 8), **Anforderungen an den Zertifizierungsprozess** (Punkt 9) und Managementsystemanforderungen (Punkt 10).

(1) Personenzertifikate

Eine Zertifizierungsstelle muss allen zertifizierten Personen ein **Zertifikat** ausstellen, welches *„in Form eines Schreibens, einer Karte oder **eines anderen Mediums** ausgestellt sein [kann]“*.[17] Das Zertifikat muss von einem Verantwortlichen des Personals der Zertifizierungsstelle unterschrieben oder autorisiert sein und **mindestens die folgenden Angaben** enthalten:

„a) den Namen der zertifizierten Person;

b) eine eindeutige Kennzeichnung;

c) den Namen der Zertifizierungsstelle;

d) einen Verweis auf das Zertifizierungsprogramm, die Norm oder andere relevante Dokumente, einschließlich das Ausstellungsdatum, falls relevant;

e) den Geltungsbereich der Zertifizierung, einschließlich Gültigkeitsbedingungen und Einschränkungen, falls zutreffend;

f) das Ausstellungs- und Ablaufdatum der Zertifizierung.“[18]

Die Personenzertifikate müssen so gestaltet werden, dass Fälschungsrisiken verringert werden.[19]

(2) Anforderungen an öffentliche Informationen

Die Zertifizierungsstelle muss **Aufzeichnungen** zu Antragstellern, Kandidaten und zertifizierten Personen führen, die Bestätigung des Status einer zertifizierten Person ermöglichen und darlegen, dass der Zertifizierungs- bzw. Rezertifizierungsprozess wirksam erfüllt worden ist.[20] Diese Aufzeichnungen müssen in einer Art und Weise identifiziert, verwaltet und vernichtet werden, dass sichergestellt ist, dass die Integrität des Verfahrens und die Vertraulichkeit der Information gewahrt bleiben und *„müssen für eine **angemessene Zeit aufbewahrt werden, für mindestens einen kompletten Zertifizierungszyklus**, oder mindestens so lange, wie es von Anerkennungsvereinbarungen, vertraglichen, rechtlichen oder anderen Verpflichtungen gefordert wird“*.[21] Der Zertifizierungszyklus kann – je nach der Zertifizierung – etwa zwei, drei, fünf

---

[17] ISO 17024, Punkt 9.4.7 (Hervorhebung durch die Autoren); ein Zertifikat wird gemäß Punkt 3.5 definiert als *„Dokument, ausgestellt durch eine Zertifizierungsstelle gemäß den Bestimmungen dieser Internationalen Norm, das angibt, dass die genannte Person die Zertifizierungsanforderungen (3.3) erfüllt“*.

[18] ISO 17024, Punkt 9.4.7 und 9.4.8.

[19] ISO 17024, Punkt 9.4.9.

[20] ISO 17024, Punkt 7.1.1.

[21] ISO 17024, Punkt 7.1.2 (Hervorhebung durch die Autoren).

oder zehn Jahre betragen. Diese Aufzeichnung stellen die Grundlage für die Zurverfügungstellung der öffentlichen Informationen dar.

In Erfüllung ihrer **Informationspflichten** muss die Zertifizierungsstelle nicht nur Informationen zum Anwendungsbereich eines Zertifizierungsprogramms, eine Liste der Voraussetzungen für das Zertifizierungsprogramm und eine allgemeine Beschreibung des Zertifizierungsprozesses öffentlich bereitstellen,[22] sondern auch *„**auf Anfrage** prüfen und darüber **informieren, ob eine Person eine aktuelle, gültige Zertifizierung in einem bestimmten Zertifizierungsbereich besitzt**, sofern eine gesetzliche Regelung die Veröffentlichung nicht verbietet“*.[23] Da jede interessierte Person eine Anfrage an die Zertifizierungsstelle richten kann und einen Anspruch auf deren Beantwortung hat, ohne ein (materielles) Rechtsinteresse oder Ähnliches nachweisen zu müssen, handelt es sich, um eine **Pflicht, die Informationen über aktuelle und gültige Personenzertifikate öffentlich zur Verfügung zu stellen**. Die Zertifizierungsstellen sind nach ISO 17024 hingegen nicht verpflichtet, über nicht mehr gültige Personenzertifikate Auskunft zu geben.

Die Informationen, die durch die Zertifizierungsstelle bereitgestellt werden, *„müssen zutreffend und dürfen nicht irreführend sein“*.[24] Neben dem Richtigkeitsgebot und Irreführungsverbot, ist aus dieser Anordnung auch ein **Vollständigkeitsgebot** abzuleiten, weshalb den anfragenden Personen sämtliche Informationen zur Verfügung zu stellen sind, die diese benötigen, um sich ausreichend über eine aktuelle und gültige Zertifizierung zu informieren. Die Informationspflicht umfasst daher (zumindest) **die Angaben, welche den Mindestinhalt eines Personenzertifikats darstellen** (vgl. oben Punkt 4.a)ii)(1)).

(3) Gegenwärtige Praxis der Zertifizierungsstellen für Personen

Die ISO 17024 schreibt nicht vor, wie die Informationen der Öffentlichkeit (technisch) zur Verfügung zu stellen sind. Die Zertifizierungsstellen bieten in der Regel an, die von ihnen ausgestellte Zertifikate telefonisch oder per Email abzufragen.

Zusätzlich bieten bereits derzeit einige Zertifizierungsstellen eine online Abfragemöglichkeit mittels einer „**Zertifikatsdatenbank**“ an.[25] Soweit ersichtlich, entsprechen die in den verfüg-

[22] ISO 17024, Punkt 7.2.2 und 7.2.3.
[23] ISO 17024, Punkt 7.2.1 (Hervorhebung durch die Autoren); denkbar wäre eine Einschränkung aus Gründen der nationalen oder öffentlichen Sicherheit, nicht aber aufgrund des Rechts auf Datenschutz oder des Amtsgeheimnisses.
[24] ISO 17024, Punkt 7.2.4.
[25] Vgl. WIFI Zertifikatsdatenbank, http://zertifizierung.wifi.at/zertifizierungwifiat/personenzertifkate/zertifikatsdatenbank/zertifikatsdatenbank; Austrian Standards Zertifikatsdatenbank, https://certificates.austrian-standards.at/searchPerson; Quality Austria - Trainings, Zertifizierungs und Begutachtungs GmbH, Personenzertifizierung, Suche nach Personenzertifikaten, https://www.qualityaustria.com/index.php?id=799&L=0; Zertifikatssuche der TÜV AUSTRIA Group, https://www.tuv.at/zertifikate-pruefen/.

baren Zertifikatsdatenbanken abrufbaren Informationen dem Mindestinhalt eines Personenzertifikats (vgl. zur Anforderungen an die Zurverfügungstellung von Informationen unten Punkt 4.e)i)).

b) Personenbezug der in der Blockchain gespeicherten Daten

Als Vorfrage ist zu klären, ob die datenschutzrechtlichen Vorschriften auf die Abbildung und Beauskunftung von Zertifikaten in der Blockchain im Rahmen des Pilotprojekts anwendbar sind. Da die DSGVO für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten gilt, hängt dies vom Personenbezug der in der Blockchain gespeicherten Daten ab.

Nach Art 4 Nr 1 DSGVO sind personenbezogene Daten *„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."*[26]

Maßgebend ist, dass die Person, auf die sich die Daten beziehen, dem Verantwortlichen bekannt oder zumindest von ihm ermittelbar ist („Ermittelbarkeit").[27]

i) Zertifikatsdaten, die in der Blockchain gespeichert werden

Abhängig von der konkreten Blockchain (bzw. der Distributed ledger technology) Anwendung können **die in den einzelnen Datenblöcken gespeicherten Informationen** personenbezogene Daten enthalten. Im Rahmen des Pilotprojekts sollten die in einem aktuellen und gültigen Personenzertifikat enthaltenen Informationen, d.h. (wenigstens) die oben geschilderten Mindestangaben, welche grundsätzlich personenbezogene Daten darstellen (können), in der Blockchain gespeichert werden („**Zertifikatsdaten**", vgl. Punkt oben 4.a)ii) und Punkt unten 4.c)iv)).

Die Zertifikatsdaten können in den Blöcken in Form des Klartexts (*plain text*), in verschlüsselter Form (*encrypted data*) oder in gehashter Form (*hashed data*) gespeichert werden.[28]

---

[26] Vgl. auch *Artikel-29-Datenschutzgruppe*, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten", WP136 (Angenommen am 20. Juni 2007).

[27] *Gola* in Gola, DS-GVO (2.Aufl., 2018) Art 4 Rz 16. Zur Identifizierbarkeit bzw. Ermittelbarkeit vgl. ErwGr 26 Satz 3 und 4 DSGVO.

[28] *Finck*, Blockchains and Data Protection in the European Union, Max Planck Institute for Innovation and Competition Research Paper No. 18-01, 10.

Da die DSGVO nicht die Verarbeitung anonymer Daten betrifft,[29] ist zu untersuchen, ob eine der Speicherungsformen die Zertifikatsdaten ausreichend anonymisiert, um den Personenbezug auszuschließen.

Konkret bestimmt die DSGVO, dass *„[d]ie Grundsätze des Datenschutzes […] nicht für anonyme Informationen gelten [sollten], 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."*[30] Die Anonymisierung ist das Ergebnis der Verarbeitung personenbezogener Daten mit dem Ziel, eine **Identifizierung unwiderruflich unmöglich zu machen**.[31]

Werden die Zertifikatdaten im Klartext auf der Blockchain gespeichert, bleiben diese personenbezogene Daten.[32] Ebenso führt eine dem Stand der Technik entsprechende Verschlüsselung, die zwar dem Datenschutz dienlich ist, indem sie bewirkt, dass die Daten für Dritte, die den Schlüssel nicht kennen, unverständlich sind, nicht zwangsläufig zu einer Anonymisierung. *„Solange der Schlüssel oder die Originaldaten verfügbar sind (wenn auch nur für eine vertrauenswürdige dritte Partei, mit der die sichere Hinterlegung von Schlüsseln vertraglich vereinbart wurde), ist die Möglichkeit der Identifizierung einer betroffenen Person nicht zuverlässig ausgeschlossen"*, weil mit dem richtigen Schlüssel der Zugriff auf die verschlüsselten Daten möglich bleibt.[33] Bei Verschlüsselung handelt es sich um eine Pseudonymisierungsmaßnahme. Auch die Verwendung von verschiedenen Hashfunktionen wird als Pseudonymisierungsmaßnahme angesehen, weil die Verbindung der gehashten Daten zu einer betroffenen Person noch immer möglich bleibt.[34] **Im Ergebnis** bleiben die Zertifikatsdaten nach deren Speicherung in der Blockchain **personenbezogene Daten**, daher sind die datenschutzrechtlichen Vorschriften anwendbar.[35]

ii) Identifikationsnummern der Teilnehmer und Zertifikatnummern

Die Teilnehmer des Blockchain-Systems und die Personenzertifikate werden in zwei verschiedenen Ästen (*streams*) der Blockchain gespeichert. Jeder schreibende und nicht schreibende Teilnehmer des Blockchain-Systems (vgl. unten Punkt 4.c)ii)) erhält eine **Identifikationsnummer** (*identifiers of participants*) bestehend aus einer Reihe von alphanumerischen Zeichen, welche den „öffentlichen Schlüssel" (*public key*) darstellen.[36]

---

[29] ErwGr 26 Satz 6 DSGVO.
[30] ErwGr 26 Satz 5 DSGVO.
[31] *Artikel-29-Datenschutzgruppe*, Stellungnahme 5/2014 zu Anonymisierungstechniken, WP216 (Angenommen am 10. April 2014), 3.
[32] *Finck*, Blockchains and Data Protection in the European Union, 10.
[33] *Artikel-29-Datenschutzgruppe*, Stellungnahme 5/2014 zu Anonymisierungstechniken, WP216, 36.
[34] *Artikel-29-Datenschutzgruppe*, Stellungnahme 5/2014 zu Anonymisierungstechniken, WP216, 24f.
[35] *Finck*, Blockchains and Data Protection in the European Union, 11.
[36] *Commission Nationale de l'Informatique et des Libertés („**CNIL**")*, Blockchain, Solutions for a responsible use of the blockchain in the context of personal data (06.11.2018), 6.

Ferner erhält jedes Personenzertifikat, das in der Blockchain gespeichert wird, zu Zwecken der Zertifikaterkennung eine kryptografische Eintragsnummer („**Zertifikatnummer**"), die wiederum im anderen Ast der Blockchain als „öffentlicher Schlüssel" (*public key*) dient.

Da die jeweilige Identifikationsnummer oder Zertifikatsnummer (zumindest) von der Stelle, die sie generiert bzw. vergeben hat, einem Teilnehmer oder einer zertifizierten Person zugeordnet werden kann, sind auch die Identifikationsnummern und Zertifikatsnummern **personenbezogene Daten**.[37]

c) Verarbeitungstätigkeit „Zentrale Datenbank für Personenzertifikate"

Im Rahmen des Pilotprojekts soll ein Blockchain-System entstehen, (i) in dem die von verschiedenen Zertifizierungsstellen für Personen ausgestellten Zertifikate digital abgebildet werden und (ii) das als einheitliche Datenbank zu deren Beauskunftung, inklusive Suche und Validierung, dienen wird. Es soll sich somit um **eine zentrale Datenbank für Personenzertifikate aller Zertifizierungsstellen für Personen** handeln.

i) Zweck der Datenverarbeitung

Personenbezogene Daten müssen für festgelegte, eindeutige und legitime Zwecke erhoben und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden.[38] Diese Zwecke sollten zum Zeitpunkt der Erhebung der personenbezogenen Daten feststehen.[39]

Die Verarbeitung von personenbezogenen Daten im Rahmen des Betriebs der zentralen Datenbank für Personenzertifikate wird zum Zwecke der möglichst effizienten **Erteilung von Auskünften über Personenzertifikate an die Öffentlichkeit** entsprechend der Anforderungen an öffentliche Informationen gemäß ISO 17024 erfolgen (vgl. Punkt 4.a)ii)(2)). Um diesen Zweck zu verwirklichen und die Beauskunftung von Personenzertifikaten wesentlich zu vereinfachen und zu beschleunigen, ist zugleich das Ziel des Pilotprojekts.

Da Personenzertifikate nicht nur in Form eines *„Schreibens"* oder einer *„Karte"*, sondern auch in Form *„eines anderen Mediums"* ausgestellt werden können (vgl. Punkt 4.a)ii)(1) oben),[40] wäre es unseres Erachtens (zukünftig) möglich, die Blockchain auch zum Zwecke der Ausstellung von Personenzertifikaten einzusetzen.

---

[37] Vgl. Art 4 Nr 1 DSGVO; *Finck*, Blockchains and Data Protection in the European Union, 13; *CNIL*, Blockchain, 6.
[38] Art 5 Abs 1 lit b DSGVO.
[39] ErwGr 39 Satz 6 DSGVO, vgl. zur Zweckbindung *Artikel-29-Datenschutzgruppe*, Opinion 03/2013 on purpose limitation, WP203 (Adopted on 2 April 2013).
[40] ISO 17024, Punkt 9.4.7 (Hervorhebung durch die Autoren); ein Zertifikat wird gemäß Punkt 3.5 definiert als *„Dokument, ausgestellt durch eine Zertifizierungsstelle gemäß den Bestimmungen dieser Internationalen Norm, das angibt, dass die genannte Person die Zertifizierungsanforderungen (3.3) erfüllt"*.

ii) Teilnehmer des Blockchain-Systems

Als *mögliche* Teilnehmer des Blockchain-Systems und somit der zentralen Datenbank für Personenzertifikate kommen die Akkreditierung Austria (Organisationseinheit des BMDW), die Zertifizierungsstellen für Personen, die Interessenvertretungen (WKÖ, AK, usw) sowie die Nutzer der Zertifikate, wie allfälligen Serviceanbieter, als Auskunftsstellen für die Öffentlichkeit und eine Art „Gatekeeper" des Blockchain-Systems, und/oder interesseierte Unternehmen und Personen, die sich an dem System beteiligen wollen (etwa Generalunternehmer im Baubereich), in Frage.

Bei der prototypischen Implementierung durch die AustriaPro werden die Teilnehmer **unterschiedliche Rollen im Blockchain-System** erhalten, was auch zu unterschiedlichen Berechtigungen und Zugriffsmöglichkeiten, voraussichtlich über eine Web-Oberfläche, führen wird. Zwar sollte jeder Teilnehmer einen Blockchain-Knoten (*Node*) betreiben, allerdings wird – entsprechend den gesetzlichen und normativen Grundlagen der Personenzertifizierung – nur gewissen Teilnehmern, nämlich den Zertifizierungsstellen für Personen, hinsichtlich den von ihnen ausgestellten Zertifikate, und der Akkreditierung Austria, hinsichtlich der Profile und der Zulassung der anderen Teilnehmer, die Möglichkeit zukommen, in die Blockchain zu schreiben (*„schreibende Teilnehmer"*).

Bei dem geplanten Blockchain-System handelt sich um eine **zulassungsbeschränkte Blockchain**. Die Definition der Rollen der Teilnehmer, insbesondere Berechtigungen, Zugriffsmöglichkeiten und Zulassung zum Blockchain-System, und die Zuteilung der beschriebenen Rollen können entweder (i) durch eine zu schaffenden allgemeinen Rechtsgrundlage, wie etwa eine **Verordnung** der Bundesministerin für Digitalisierung und Wirtschaftsstandort oder (wohl auch) Leitfäden der Akkreditierung Austria, oder **alternativ** (ii) durch Abschluss einer **Vereinbarung** zwischen den Teilnehmern des Blockchain-Systems bzw. später durch den Beitritt zu einer solchen Vereinbarung erfolgen. Aufgrund der vorgesehenen Regelung kann die Zuteilung der Rolle und die Zulassung zum Blockchain-System im konkreten Einzelfall etwa auf einer individuellen Entscheidung, seitens etwa Akkreditierung Austria, basieren. Durch diese Regelung ist **sicherzustellen, dass sich sämtliche Blockchain-Knoten in der EU befinden werden** und kein Datentransfer außerhalb der EU erfolgen wird. Ansonsten muss zusätzlich eine Rechtgrundlage für die Übermittlung von personenbezogenen Daten an das jeweilige Drittland, in dem sich (zumindest) ein Teilnehmer befindet, vorgesehen werden.[41]

[41] Art 44 DSGVO, vgl *CNIL*, Blockchain, 5.

iii) Verarbeitungsvorgänge

Unter einer „Verarbeitung“ ist jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten zu verstehen, wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.[42] Aus datenschutzrechtlicher Sicht ist der Betrieb einer zentralen Zertifikatsdatenbank als eine Reihe von Verarbeitungsvorgängen anzusehen.

Einerseits werden die aktuellen, gültigen Zertifikate – soweit dies noch nicht erfolgt ist – digitalisiert, die Zertifikatsdaten in einem einheitlichen Blockchain-System zusammengeführt und **in der Blockchain selbst (*on chain*) gespeichert**. Anderseits werden die neu ausgestellten Personenzertifikate dieser Blockchain hinzugefügt.

Die in der Blockchain gespeicherten **Zertifikatsdaten** werden in Rahmen der **Beauskunftung** von Zertifikaten von der Akkreditierung Austria, den Zertifizierungsstellen, und allfälligen Serviceanbietern (siehe gleich unten) gesucht, validiert und den interessierten Personen zum Abruf etwa über eine Web-Oberfläche bereitgestellt oder sonst übermittelt (z.B. Übermittlung von Zertifikatsbescheinigungen als PDF-Datei).

Um die Einsicht in die Datenbank auch den Personen, die keinen Blockchain-Knoten betreiben und daher keinen Teilnehmer des Blockchain-Systems sind, zu ermöglichen, wird es sich bei der Blockchain um eine **öffentlich einsehbare Blockchain** (*open Blockchain*) handeln. **Alternativ** ist möglich, etwa wenn es sich in weiteren Verlauf des Projekts herausstellt, dass dies technisch nicht umsetzbar oder sonst unerwünscht sei, spezielle **Serviceanbieter** als Auskunftsstellen für die interessierte Öffentlichkeit und damit eine Art „Gatekeeper“ der (nicht öffentlich einsehbaren) Blockchain einzusetzen. Deren Rolle als Teilnehmer des Blockchain-Systems, insbesondere Berechtigungen, Zugriffsmöglichkeiten und die Zulassung, wären genau zu definieren (vgl. oben Punkt 4.c)ii)).

iv) Kategorien personenbezogener Daten

Verschiedene (potentielle) Teilnehmer werden, abhängig von deren Rolle im Blockchain-System, unterschiedliche Verarbeitungsvorgänge vornehmen und dabei unterschiedliche Kategorien der personenbezogenen Daten verarbeiten.

Die Akkreditierungsstelle **Akkreditierung Austria** wird auf (i) Stammdaten der Zertifizierungsstellen für Personen (ID, Bezeichnung, Adresse, Webseite, Datum der Akkreditierung) und auf

[42] Art 4 Nr 2 DSGVO.

Angaben zu den Zertifikatstypen, zur deren Ausstellung die jeweilige Zertifizierungsstelle berechtigt ist (Bezeichnung und Code der Zertifizierung), sowie Stammdaten von anderen allfälligen Systemteilnehmern, wie etwa Serviceanbieter, zugreifen können.[43] Des Weiteren wird die Akkreditierung Austria (ii) alle von verschiedenen Zertifizierungsstellen ausgestellten Personenzertifikate gegenüber interessierten Unternehmen und Personen beauskunften sowie (iii) die Berichte über die Verwendung der zentralen Datenbank für Personenzertifikate erstellen können.

Die **Zertifizierungsstellen** für Personen werden (i) Zertifikate in die Blockchain speichern. Die Personenzertifikate enthalten **Zertifikatsdaten** (vgl. oben Punkt 4.b)i)) bestehend aus (a) Angaben über den Aussteller, d.h. die Stammdaten der ausstellenden Zertifizierungsstelle (siehe oben), (b) Angaben über die zertifizierten Person (Titel vorangestellt, Vorname, Familienname, Titel nachgestellt) und (c) Angaben über das Zertifikat selbst (Zertifikatsnummer, Bezeichnung und Code der Zertifizierung sowie Datum der Ausstellung und des Ablaufs der Gültigkeit). Die Zertifizierungsstellen können ferner (ii) eigene sowie von anderen Zertifizierungsstellen ausgestellten Personenzertifikate, die in der Blockchain gespeichert sind, beauskunften.

Wird die zentrale Datenbank für Personenzertifikate nicht etwa über eine Web-Oberfläche öffentlich zugänglich gemacht, besteht – wie oben ausgeführt – die Möglichkeit, der Öffentlichkeit den Zugang zu den Zertifikatsdaten über spezielle **Serviceanbieter** zu ermöglichen. Diese wären befugt, sämtliche Personenzertifikate (i) zu beauskunften.

Sämtliche Teilnehmer des Blockchain-Systems verarbeiten auch **Identifikationsnummern** der jeweils anderen Teilnehmer.

Zu betonen ist, dass beim Betrieb der zentralen Datenbank für Personenzertifikate **keine besonderen Kategorien** von personenbezogener Daten im Sinne vom Art 9 DSGVO verarbeitet werden sollen.

v) Datenminimierung

Der Grundsatz der Datenminimierung ist ein leitendes Prinzip des Datenschutzrechts, das wesentlich zum Schutz der Interessen der betroffenen Personen beiträgt. Der Datenminimierung entsprechend müssen personenbezogene Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein.[44] Die Angemessenheit, die Erheblichkeit und die Beschränkung auf das notwendige Maß der geplanten Datenverarbeitung sind **am Verarbeitungszweck der zentralen Datenbank für Personenzertifikate zu messen**.[45] Dieser ist die effiziente Erteilung von Auskünften über Personenzertifikate an die

[43] Diese Informationen sind als personenbezogene Daten der Zertifizierungsstellen (noch) nach § 1 DSG geschützt.
[44] Art 5 Abs 1 lit c DSGVO.
[45] *Hötzendorfer/Tschohl/Kastelitz* in Knyrim, DatKomm Art 5 DSGVO (Stand 1.10.2018, rdb.at) Rz 35.

Öffentlichkeit entsprechend der Anforderungen an öffentliche Informationen gemäß ISO 17024 (vgl. oben 4.c)i)).

Die Verarbeitung von personenbezogenen Daten im Rahmen des Betriebs der zentralen Datenbank für Personenzertifikate ist daher auf die personenbezogenen Daten zu beschränken, die (i) zur Beauskunftung der Personenzertifikate erforderlich sind oder (ii) zum Betrieb bzw. zur Funktionsfähigkeit der zentralen Datenbank für Personenzertifikate erforderlich sind.

Zu (i) einer der ISO 17024 entsprechenden Beauskunftung der Personenzertifikate sind (zumindest) **die Angaben über aktuelle und gültige Personenzertifikate im Umfang des Mindestinhalts eines Personenzertifikats** erforderlich. Hingegen verlangt die ISO 17024 nicht die Beauskunftung von abgelaufenen Zertifikaten. Da diesbezüglich keine Informationspflicht (mehr) besteht, ist die Verarbeitung, der in diesen Zertifikaten enthaltenen personenbezogenen Daten zu unterlassen (vgl. oben 4.a)ii)(2)).

Der (ii) Betrieb bzw. Funktionsfähigkeit der zentralen Datenbank für Personenzertifikate erfordert die Verarbeitung von Identifikationsnummern der Teilnehmer (vgl. oben 4.b)ii)) sowie gegenseitigen Zugriff auf die von den anderen Zertifizierungsstellen ausgestellten Zertifikate und die darin enthaltene personenbezogen Daten für Zwecke der Beauskunftung gegenüber der interessierten Unternehmen und Personen.

d) Datenschutzrechtliche Verantwortlichkeit

Da der Verantwortliche zur Einhaltung der Grundsätze für die Verarbeitung personenbezogener Daten verpflichtet ist und sich die Rechte der betroffenen Personen gegen ihn und nicht etwa gegen Auftragsverarbeiter richten,[46] ist im nächsten Schritt zu untersuchen, wer in der oben beschriebenen Blockchain-basierten zentralen Datenbank für Personenzertifikate als Verantwortlicher anzusehen ist.

Die datenschutzrechtliche Verantwortlichkeit stellt in einem dezentral organisierten System eine Herausforderung dar, weil eine Vielzahl von beteiligten Akteuren als Verantwortlicher in Betracht kommt und sie somit von der Governance-Struktur des jeweiligen Blockchain-Systems abhängt.[47]

i) (Gemeinsam) Verantwortliche

Der Verantwortlicher ist *„die natürliche oder juristische Person […], die allein oder gemeinsam mit anderen **über die Zwecke und Mittel der Verarbeitung** von personenbezogenen Daten*

[46] *Bertermann* in Ehmann/Selmayr, DS-GVO[2] Art 28 Rz 27.
[47] *Martini/Weinzierl*, Die Blockchain-Technologie und das Recht auf Vergessenwerden, NVwZ 2017, 1251 (1253); *Finck*, Blockchains and Data Protection in the European Union, 18.

***entscheidet** […]"*.[48] Dieser Begriff ist *„ein funktionelles Konzept, das die Zuweisung der Verantwortlichkeiten anhand des **tatsächlichen Einflusses** und damit auf der Grundlage einer Analyse der Fakten und nicht einer formellen Analyse ermöglichen soll"*.[49]

In einem Blockchain-System entscheiden grundsätzlich die Teilnehmer über die Zwecke, die durch die Verarbeitung verfolgt werden, und die Mittel der Verarbeitung, unter anderem Einsatz der Blockchain-Technologie. Als Verantwortliche sind die **schreibenden Teilnehmer** anzusehen, die berechtigt sind in die Blockchain zu schreiben und somit neue (personenbezogene) Daten in die Datenbank einzutragen.[50]

Im Pilotprojekt fungiert die **Akkreditierung Austria** als die organisierende Einheit, die unter anderem über die über Zugangsrechte zur zentralen Datenbank für Personenzertifikate und somit zur Blockchain entscheiden wird. Da sie auch die zentrale Zulassungsverwaltung betreiben wird, ist sie wegen ihren tatsächlichen Einflusses auf die Gestaltung der zentralen Datenbank für Personenzertifikate als Verantwortliche anzusehen.

Ferner werden die **Zertifizierungsstellen für Personen** berechtigt, Zertifikate auszustellen und diese in die zentrale Datenbank für Personenzertifikate einzutragen. Da Sie berechtigt werden in die Blockchain zu schreiben und diese dadurch zu beeinflussen, sind sie als Verantwortliche anzusehen.

Legen zwei oder mehr Verantwortliche gemeinsam die Zwecke der und die Mittel zur Verarbeitung fest, so sind sie **gemeinsam Verantwortliche**.[51] Dies ist auch grundsätzlich der Fall, wenn sich mehrere Teilnehmer entscheiden, die Verarbeitung in einer Blockchain gemeinsam durchzuführen.[52] Sie müssen in einer Vereinbarung in transparenter Form festlegen, wer von ihnen welche Verpflichtung gemäß der DSGVO erfüllt, insbesondere was die Wahrnehmung der Rechte der betroffenen Person angeht, und wer welchen Informationspflichten gemäß den Artikeln 13 und 14 DSGVO nachkommt.[53] Diese Vereinbarung muss *„die jeweiligen tatsächlichen Funktionen und Beziehungen der gemeinsam Verantwortlichen gegenüber betroffenen Personen gebührend widerspiegeln"* und ist in ihren wesentlichen Teilen der betroffenen Personen zur Verfügung zu stellen.[54]

Die Akkreditierung Austria und die Zertifizierungsstellen für Personen haben daher eine **Vereinbarung** abzuschließen, welche die Entscheidungsbefugnis der einzelnen Verantwortlichen hinsichtlich der Zwecke und der Mittel der Vereinbarung sowie die Aufgabenverteilung hinsichtlich der gesetzlichen Pflichten nach der DSGVO enthält.[55] Neue schreibende Teilnehmer könnten dieser Vereinbarung bei deren Zulassung zum Blockchain-System beitreten.[56]

---

[48] Art 4 Nr 7 DSGVO.
[49] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter", WP169 (Angenommen am 16. Februar 2010), 12.
[50] *CNIL*, Blockchain, 1.
[51] Art 26 Abs 1 Satz 1 DSGVO.
[52] *CNIL*, Blockchain, 2.
[53] Art 26 Abs 1 Satz 2 DSGVO.
[54] Art 26 Abs 2 DSGVO.
[55] *Piltz* in Gola, DS-GVO[2] Art 26 Rz 20.
[56] *Schrey/Thalhofer*, Rechtliche Aspekte der Blockchain, NJW 2017, 1431 (1434).

Eine Vereinbarung ist allerdings nicht erforderlich, *„sofern und soweit die jeweiligen Aufgaben der Verantwortlichen […] durch Rechtsvorschriften der Union oder der Mitgliedstaaten, denen die Verantwortlichen unterliegen, festgelegt sind“*.[57] Die Vereinbarung zwischen der Akkreditierung Austria und den Zertifizierungsstellen für Personen könnte daher durch eine (inhaltlich entsprechend gestaltete) **Verordnung** der Bundesministerin für Digitalisierung und Wirtschaftsstandort ersetzt werden. Wohl zu verneinen ist hingegen die Frage, ob den Leitfäden der Akkreditierung Austria die erforderliche Rechtsqualität und Rechtsbindungswirkung zukommt, um diese als Rechtsvorschrift des Mitgliedstaats Österreich im Sinne der DSGVO qualifizieren zu können, daher kann deren Erlass die Vereinbarung zwischen gemeinsam Verantwortlichen nicht ersetzen.

Alternativ ist möglich, dass die schreibenden Teilnehmer des Blockchain-Systems vor der Aufnahme der Verarbeitung der personenbezogenen Daten ***den* Verantwortlichen identifizieren**, indem sie für die Verarbeitung etwa (i) eine eigene juristische Person gründen, beispielsweise einen **Verein** oder eine GmbH, oder (ii) einen Teilnehmer als Verantwortlichen benennen, der sämtliche Entscheidungen im Zusammenhang mit der Verarbeitung in der Blockchain für alle Verantwortliche trifft.[58] Diese **Benennung** kann wiederum durch eine (Register-)Verordnung der Bundesministerin für Digitalisierung und Wirtschaftsstandort oder eine Vereinbarung zwischen den Teilnehmern getroffen werden (welche allenfalls als GesbR zu qualifizieren wäre).

Andere schreibende Teilnehmer wären in diesen Fällen als Auftragsverarbeiter anzusehen, weil sie die personenbezogenen Daten im Auftrag der gegründeten juristischen Person oder des benannten Verantwortlichen verarbeiten würden.[59]

ii) Auftragsverarbeiter

Ein Auftragsverarbeiter ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.[60] Diese Verarbeitungstätigkeit kann auf eine sehr spezifische Aufgabe oder einen sehr spezifischen Kontext beschränkt oder allgemeiner und weiter gefasst sein.[61]

Bei der Bestimmung der tatsächlichen Beziehungen zwischen den verschiedenen Teilnehmern ist ein **funktioneller Ansatz** maßgebend und daher die Art der Entscheidung über Zwecke und Mittel der Verarbeitung zu analysieren. Im Kontext des Datenschutzrechts ist es die Aufgabe

[57] Art 26 Abs 1 Satz 2 DSGVO.
[58] *CNIL*, Blockchain, 2f.
[59] *CNIL*, Blockchain, 3f; Art 4 Nr 8 DSGVO.
[60] Art 4 Nr 8 DSGVO.
[61] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher“ und „Auftragsverarbeiter“, WP169, 30.

eines Auftragsverarbeiters, die vom Verantwortlichen erteilten Weisungen zumindest hinsichtlich des Zwecks der Verarbeitung und der wesentlichen Elemente der Mittel zu befolgen.[62]

Bei zulassungsbeschränkten Blockchain-Systemen sind die Teilnehmer, die nicht als organisierende Einheit auftreten, also „einfache" Betreiber von Blockchain-Knoten (*Nodes*) grundsätzlich als Auftragsverarbeiter anzusehen.[63] Beim Betrieb der zentralen Datenbank für Personenzertifikate werden der Zweck und die Mittel der Datenverarbeitung von den schreibenden Teilnehmern, d.h. der Akkreditierung Austria und den Zulassungsstellen für Personenzertifizierung, bzw. einer von denen gegründeten juristischen Person oder einem von denen benannten Verantwortlichen festgelegt, nicht aber von **nicht-schreibenden Teilnehmern, die „einfache" Betreiber von Blockchain-Knoten sind**. Diese sind daher als Auftragsverarbeiter zu qualifizieren.

Ferner können bei zulassungsbeschränkten Blockchain-Systemen die Schürfer (*Miners*) grundsätzlich als Auftragsverarbeiter angesehen werden.[64] Im Blockchain-System der zentralen Datenbank für Personenzertifikate besteht allerdings keine eigenständige Rolle für Schürfer (*Miner*), weil die schreibenden Teilnehmer diese Rolle selbst übernehmen und neue Blöcke nach einem Rundlauf-Verfahren (*round-robin*) generieren. Dabei machen sich alle beteiligten Knoten per Protokoll eine Reihenfolge aus, daher wird jeder Knoten in dieser Reihenfolge in einer definierten Zeitspanne herangezogen.

Die Verarbeitung durch einen Auftragsverarbeiter erfolgt „*auf der Grundlage eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, der bzw. das den Auftragsverarbeiter in Bezug auf den Verantwortlichen bindet und in dem Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Pflichten und Rechte des Verantwortlichen festgelegt sind*".[65] Daher sind schreibende Teilnehmer verpflichtet, mit den sonstigen Teilnehmern jeweils eine **Auftragsverarbeitungsvereinbarung** abzuschließen, bevor diese zum Blockchain-System zugelassen werden.

Alternativ ist auch möglich, die Öffnungsklausel für mitgliedstaatliche Regelungen zu nützen und die Auftragsverarbeitung in einem *„anderen Rechtsinstrument nach […] dem Recht der Mitgliedstaaten"* zu regeln. Die Mitgliedstaaten können eine andere Gestaltungsform für die Rechtsbeziehungen zwischen Verantwortlichem und Auftragsverarbeiter vorsehen und sind bei der Auswahl der rechtlichen Handlungsinstrumente frei diese selbst und autonom zu regeln.[66] Erforderlich ist jedoch, dass eine rechtliche Bindung des Auftragsverarbeiter an den

---

[62] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter", WP169, 31, 33.

[63] *Martini/Weinzierl*, Die Blockchain-Technologie und das Recht auf Vergessenwerden, NVwZ 2017, 1251 (1254), ihnen folgend *bitkom*, Faktenpapier - Blockchain und Datenschutz (Dokumentversion 1.1, Aktualisiert am 05.04.2018) 30; *Finck*, Blockchains and Data Protection in the European Union, 18.

[64] *CNIL*, Blockchain, 2f.

[65] Art 28 Abs 3 DSGVO.

[66] *Spoerr* in Wolff/Brink, BeckOK Datenschutzrecht (25. Edition, Stand: 01.08.2018) Art 28 Rz 46.

Verantwortlichen erzeugt wird.[67] Diese Rechtsbindungswirkung könnte etwa durch eine **Verordnung** der Bundesministerin für Digitalisierung und Wirtschaftsstandort erzeugt werden. Diese Verordnung müsste jedoch den gleichen Regelungsinhalt aufweisen wie ein Auftragsverarbeitungsvertrag.[68]

Ferner ist es im Lichte des Datenminimierungsgrundsatzes und wegen der praktischen Durchsetzbarkeit der datenschutzrechtlichen Vorgaben **zweckmäßig, die Anzahl der nicht-schreibenden Teilnehmer, die „einfache" Betreiber von Blockchain-Knoten sind, zu beschränken** (vgl. unten Punkt 4.f)iv)(1)(d)).

Wird (i) die im Rahmen des Pilotprojekts entwickelte Blockchain – und somit die zentrale Datenbank für Personenzertifikate – **öffentlich einsehbar**, bestünde keine Notwendigkeit, dass jedes interesseierte Unternehmen oder Person einen Blockchain-Knoten betreibt und daher als nicht-schreibende Teilnehmer des Blockchain-Systems Auftragsverarbeiter wird. Sollte dies technisch nicht umsetzbar oder sonst unerwünscht sein, (ii) wäre es möglich, **Serviceanbieter** als Auskunftsstellen für die Öffentlichkeit und eine Art „Gatekeeper" des Blockchain-Systems einzusetzen. Im letzten Fall wären Serviceanbieter „einfache" Betreiber von Blockchain-Knoten und damit Auftragsverarbeiter. **In beiden Fällen wären die interesseierten Unternehmen und Personen, welche die Auskünfte über Zertifikate erhalten, nicht als Teilnehmer des Blockchain-Systems, sondern als Empfänger der personenbezogenen Daten[69] und als Dritte[70] zu qualifizieren** (vgl. oben Punkt 4.c)iii)).

e) Rechtsmäßigkeit der Datenverarbeitung

Die Datenverarbeitung ist nur erlaubt, wenn für sie eine Legitimationsgrundlage vorliegt (*Verbot mit Erlaubnisvorbehalt*). Art 6 DSGVO listet die Erlaubnistatbestände auf, die für Daten gelten, die nicht in die Gruppe der besonderen Kategorien personenbezogener Daten[71] gehören. Die Verarbeitung ist danach rechtmäßig, wenn *„mindestens"* ein gesetzlicher Erlaubnistatbestand erfüllt ist oder die betroffene Person eingewilligt hat.[72] Da die gesetzlichen Erlaubnistatbestände grundsätzlich auch im Falle einer Verweigerung oder eines Widerrufs der Einwilligung greifen, sind diese vorab zu prüfen.[73]

---

[67] *Martini* in Paal/Pauly, DS-GVO BDSG[2] Art 28 Rz 28.
[68] *Spoerr* in Wolff/Brink, BeckOK Datenschutzrecht (25. Edition, Stand: 01.08.2018) Art 28 Rz 47.
[69] Art 4 Nr 9 DSGVO.
[70] Art 4 Nr 10 DSGVO.
[71] Art 9 DSGVO.
[72] Art 6 Abs 1 DSGVO; *bitkom*, Faktenpapier - Blockchain und Datenschutz, 30; ErwGr 40 DSGVO.
[73] *Schulz* in Gola, DS-GVO[2] Art 6 Rz 11.

i) Gesetzliche Erlaubnistatbestände

Die Verarbeitung ist rechtmäßig, wenn sie zur **Erfüllung einer rechtlichen Verpflichtung** erforderlich ist, der der Verantwortliche unterliegt.[74] Die Rechtspflicht des Verantwortlichen, welche kraft objektiven Rechts besteht, muss die Verarbeitung von konkreten personenbezogenen Daten erforderlich machen.[75] Dieser Erforderlichkeitsgrundsatz ist als Ausfluss des Zweckbindungsgrundsatzes zu verstehen und verlangt, dass die Datenverarbeitung zur Erreichung des Zwecks objektiv tauglich ist und sich auf die zur Zweckerreichung notwendige Maß beschränkt.[76]

Bei der Erfüllung einer rechtlichen Verpflichtung handelt sich jedoch nicht um einen „eigenständigen" allgemeinen Erlaubnistatbestand, dieser bedarf vielmehr einer ausfüllenden unionsrechtlichen oder mitgliedstaatlichen Norm.[77] Als Rechtsinstrument kommen neben formellen Gesetzen auch untergesetzliche Erlaubnistatbestände, vor allem Verordnungen von Verwaltungsbehörden gemäß Art 18 Abs 2 B-VG und sonstige Normen, die auf eine durch formelles Gesetz vorgegebene Ermächtigungsgrundlage zurückzuführen sind, in Betracht.[78] Welchem Rechtsgebiet die Rechtspflicht entstammt ist ohne Belang, daher sind neben den öffentlich-rechtlichen auch zivilrechtliche Vorgaben erfasst.[79]

Als Rechtsgrundlage für die Verarbeitung von personenbezogenen Daten im Rahmen des Betriebs der zentralen Datenbank für Personenzertifikate kommt **ISO 17024** als normative Grundlage in Frage, deren Rechtsverbindlichkeit auf der Anordnung im § 7 Abs 1 Z 1 AkkG fußt.[80] Danach sind Zertifizierungsstellen für Personen verpflichtet, jede interessierte Person *„auf Anfrage […] darüber informieren, ob eine Person eine aktuelle, gültige Zertifizierung in einem bestimmten Zertifizierungsbereich besitzt"*.[81] Die erteilten Informationen müssen richtig, nicht irreführend und vollständig sein, um den anfragenden Personen sämtliche Informationen zur Verfügung zu stellen sind, die diese benötigen, um sich ausreichend über eine aktuelle und gültige Zertifizierung zu informieren (vgl. oben Punkt 4.a)ii)(2)).[82] Auf welchem Weg diese Informationen der Öffentlichkeit zur Verfügung zu stellen sind, schreibt die ISO 17024

---

[74] Art 6 Abs 1 lit c DSGVO.
[75] *Kastelitz/Hötzendorfer/Tschohl* in Knyrim, DatKomm Art 6 DSGVO (Stand 1.10.2018, rdb.at) Rz 39.
[76] *Schulz* in Gola, DS-GVO[2] Art 6 Rz 20; *Heberlein* in Ehmann/Selmayr, DS-GVO[2] Art 6 Rz 17.
[77] Art 6 Abs 2 und Abs 3 DSGVO; ErwGr 41 Satz 1 DSGVO; *Schulz* in Gola, DS-GVO[2] Art 6 Rz 197.
[78] ErwGr 41 DSGVO, *Kastelitz/Hötzendorfer/Tschohl* in Knyrim, DatKomm Art 6 DSGVO (Stand 1.10.2018, rdb.at) Rz 39; *Schulz* in Gola, DS-GVO[2] Art 6 Rz 198; *Albers/Veit* in Wolff/Brink, BeckOK Datenschutzrecht (25. Edition, Stand: 01.05.2018) Art 6 Rz 58.
[79] *Schulz* in Gola, DS-GVO[2] Art 6 Rz 43.
[80] Vgl. dazu FN 10, insb. § 7 Abs 1 Z 1 AkkG iVm Mitteilung der Kommission im Rahmen der Durchführung der Verordnung (EG) Nr. 765/2008 des Europäischen Parlaments und des Rates, Beschluss Nr. 768/2008/EG des Europäischen Parlaments und des Rates, Verordnung (EG) Nr. 1221/2009 des Europäischen Parlaments und des Rates (2016/C 293/06), https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:52016XC0812(07) **und** Vorwort der ISO 17024: *„Diese Europäische Norm muss den Status einer nationalen Norm erhalten, entweder durch Veröffentlichung eines identischen Textes oder durch Anerkennung bis Januar 2013, und etwaige entgegenstehende nationale Normen müssen bis Januar 2013 zurückgezogen werden."*
[81] ISO 17024, Punkt 7.2.1.
[82] ISO 17024, Punkt 7.2.4.

zwar nicht (ausdrücklich) vor (vgl. oben Punkt 4.a)ii)(3)), allerdings muss die Art der Zurverfügungstellung von Informationen die effektive Erfüllung der geschilderten Informationspflicht ermöglichen. Die Möglichkeit bei einer Zertifizierungsstelle, die von ihr ausgestellten Personenzertifikate telefonisch oder per Email abzufragen, erfüllt (hinreichend) diese Anforderungen und stellt die zurzeit geläufigste Form der Beauskunftung dar (vgl. oben Punkt 4.a)ii)(3)). Darüber hinaus können auch andere Formen der Beauskunftung implementiert werden, die die effektive Erfüllung der Informationspflicht gewährleisten. Da eine Abfrage über eine Web-Oberfläche die effektive Erfüllung der Informationspflicht ermöglicht, ist sie mit der Abfrage per Telefon oder Email (materiell) gleichwertig. Die Pflicht, die Informationen über aktuelle und gültige Personenzertifikate der interessierten Öffentlichkeit zur Verfügung zu stellen, kann daher auch über eine **online verfügbare Datenbank** erfüllt werden. Diese Datenbank muss sämtliche Informationen enthalten, die die anfragende Person benötigt, um sich ausreichend über eine aktuelle und gültige die Zertifizierung zu informieren und umfasst daher zumindest die Angaben, welche den Mindestinhalt eines Personenzertifikats darstellen (vgl. oben Punkt 4.a)ii)). Obwohl die ISO 17024 die Schaffung einer zentralen Datenbank oder eines Registers nicht (ausdrücklich) verlangt und die Zertifizierungsstellen nicht zur Beauskunftung der von anderen Zertifizierungsstellen ausgestellten Personenzertifikate verpflichtet, entspricht eine möglichst die effektive Erfüllung der oben geschilderten Informationspflicht dem Wesen der ISO 17024. Diese kann am besten durch die Schaffung einer **zentralen Datenbank** für Personenzertifikate gewährleistet werden, deren Entwicklung die Beauskunftung wesentlich vereinfachen und beschleunigen würde. Die ISO 17024 stellt daher unseres Erachtens eine ausreichende (datenschutzrechtliche) Rechtsgrundlage für die Verarbeitung personenbezogener Daten, die zur Beauskunftung der Personenzertifikate in der zentralen Datenbank oder zum deren Funktionieren erforderlich sind (vgl. Punkt 4.c)v)).

Des Weiteren haben die Zertifizierungsstellen sowie auch die interessierten Unternehmen und Personen ein **berechtigtes Interesse** an der Beauskunftung von Personenzertifikaten in einer zentralen online verfügbaren Datenbank, weil diese die möglichst einfache und schnelle Erfüllung der Informationspflicht der Zertifizierungsstellen gewährleistet. Die Offenlegung von für die Beauskunftung und das Funktionieren der zentralen Datenbank erforderlichen personenbezogenen Daten an die Akkreditierung Austria, andere Zertifizierungsstellen und allfällige Serviceanbieter ist im Rahmen der zentralen Datenbank für Personenzertifikate notwendig. Der Aufbau einer zentralen Datenbank für Personenzertifikate werde auch nicht die Interessen oder Grundrechte und Grundfreiheiten der zertifizierten Personen als betroffenen Personen verletzen. Einerseits werden nur die bereits bisher öffentlich zugänglichen personenbezogenen Daten über Personenzertifikate enthalten. Anderseits ist vielmehr davon auszugehen, dass wegen leichterer Einsicht in die enthaltenen Zertifikate durch interessierte Unternehmen und Personen (wohl) die Interessen der zertifizierten Personen an der leichten Auffindbarkeit und Überprüfbarkeit der Personenzertifikate gefördert werden.[83] Die Verarbeitung personenbezogener Daten in der zentralen Datenbank für Personenzertifikate, die zur

[83] Vgl. Art 6 Abs 1 lit f DSGVO; dazu etwa *Kastelitz/Hötzendorfer/Tschohl* in Knyrim, DatKomm Art 6 DSGVO (Stand 1.10.2018, rdb.at) Rz 49ff mwN.

Beauskunftung der Personenzertifikate oder zum Funktionieren der Datenbank erforderlich sind, stützt sich daher zusätzlich auf die Wahrung der berechtigten Interessen der Verantwortlichen und Dritten.

Alternativ könnte nicht nur mit einem (nationalen) Gesetz, sondern auch etwa mit einer (Register-)**Verordnung** der Bundesministerin für Digitalisierung und Wirtschaftsstandort eine (i) rechtliche Verpflichtung der Zertifizierungsstellen für Personen und (möglicherweise) der Akkreditierung Austria zur Führung (bzw. zum Betrieb) einer zentralen Datenbank für Personenzertifikate und (ii) allenfalls eine Rechtspflicht der Serviceanbieter zur Teilnahme an einem solchen System eingeführt werden. Zusätzlich wäre es möglich, (iii) in dieser Verordnung auch die Verpflichtung zur Beauskunftung von nicht mehr gültigen Zertifikaten, ermöglicht durch die Verwaltung von historischen Daten in der zentralen Datenbank, vorzusehen (ähnlich wie dies im Firmenbuch der Fall ist; vlg zum Recht auf Löschung unten Punkt 4.f)iv)(3)). Ferner könnte man in dieser Verordnung in Ergänzung und/oder Präzisierung der ISO 17024 neben dem Zweck der Datenverarbeitung unter anderem auch *„die allgemeinen Bedingungen [der DSGVO] zur Regelung der Rechtmäßigkeit der Verarbeitung personenbezogener Daten [präzisieren] und [festlegen] wie der Verantwortliche zu bestimmen ist, welche Art von personenbezogenen Daten verarbeitet werden, welche Personen betroffen sind, welchen Einrichtungen die personenbezogenen Daten offengelegt, für welche Zwecke und wie lange sie gespeichert werden dürfen und welche anderen Maßnahmen ergriffen werden, um zu gewährleisten, dass die Verarbeitung rechtmäßig und nach Treu und Glauben erfolgt“*.[84] Dabei handelt sich um einen nicht abschließenden Katalog von „Kann“-Vorgaben.[85] Je sensibler der Bereich ist, in dem die Datenverarbeitung stattfindet, umso höher sind die Anforderungen an die Ausgestaltung der rechtfertigenden Norm.[86] Da die innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen ein datenschutzrechtlicher Risikofaktor ist[87], wäre wegen der Anwendung der Blockchain-Technologie bei der Implementierung der zentralen Datenbank für Personenzertifikate im Rahmen des Pilotprojekts ein höheres Determinierungsgrad zu bevorzugen.

Zu beachten ist allerdings, dass durch die spezifische Rechtsvorschrift allein die Zulässigkeit der Verarbeitung bestimmt werden kann. **Die übrigen datenschutzrechtlichen Pflichten des Verantwortlichen können nur dann geändert (und allenfalls eingeschränkt) werden, wenn diesbezüglich eine gesonderte Konkretisierungsklausel herangezogen wird** (z.B. Art 23 DSGVO hinsichtlich einer Beschränkung der Rechte der betroffenen Personen; vgl. unten Punkt 4.f)v)).[88]

---

[84] ErwGr 45 Satz 5 DSGVO.
[85] *Schulz* in Gola, DS-GVO[2] Art 6 Rz 199, 201.
[86] *Schulz* in Gola, DS-GVO[2] Art 6 Rz 199.
[87] *Artikel-29-Datenschutzgruppe*, Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt“, WP 248 Rev. 01 (zuletzt überarbeitet und angenommen am 4. Oktober 2017), 12.
[88] *Schulz* in Gola, DS-GVO[2] Art 6 Rz 42.

Ferner wäre denkbar, die zentrale Datenbank für Personenzertifikate aufgrund einer vertraglichen Vereinbarung mit zertifizierten Personen zu führen, da die Verarbeitung von personenbezogenen Daten rechtmäßig ist, wenn sie für die Erfüllung (oder den geplanten Abschluss) eines Vertrags erforderlich ist.[89] Erfolgt die Zertifizierung aufgrund eines Zertifizierungsvertrags, ist die Beauskunftung der erteilten Zertifizierung als vertragliche Nebenverpflichtung grundsätzlich zulässig, weil sie zur Zweckerreichung erforderlich ist. Ohne eine entsprechende vertragliche Ausgestaltung wäre hingegen die Beauskunftung in einer zentralen Datenbank für Personenzertifikate zur Verwirklichung des Zweckes des Zertifizierungsvertrags nicht erforderlich und daher die Datenverarbeitung bei deren Betrieb auf einen anderen Erlaubnistatbestand zu stützen oder ansonsten unzulässig.

Als dieser andere Erlaubnistatbestand käme primär die Einwilligung in Frage. Soll neben der auf vertraglicher Grundlage zulässigen zusätzlich eine einwilligungsbasierte Datenverarbeitung stattfinden, hat der Verantwortliche das Koppelungsverbot zu beachten, weshalb die Zertifizierung bzw. Abschluss des Zertifizierungsvertrags nicht von der Einwilligung in die Beauskunftung über die zentrale Datenbank für Personenzertifikate abhängig gemacht werden dürfte, weil diese Art der Beauskunftung für die Erfüllung des Zertifizierungsvertrags nicht erforderlich ist.[90] Sollte diese Einwilligung gleichzeitig mit dem Abschluss des Zertifizierungsvertrags schriftlich erfolgen („kombinierte Einwilligung"), müsste das Einwilligungsersuchen *„in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache so erfolgen, dass es von den anderen Sachverhalten klar zu unterscheiden ist"*.[91] Eine klare Unterscheidbarkeit vom Zertifizierungsvertrag könnte durch optische Hervorhebung sichergestellt werden. In der Internetkommunikation genügen gesondert anzuklickende Checkboxen in der Regel diesen Anforderungen.[92]

ii) Einwilligung

Des Weiteren ist die Verarbeitung rechtmäßig, wenn die betroffene Person ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben hat.[93] Unter Einwilligung der betroffenen Person ist jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist, zu verstehen.[94]

Um die zentrale Datenbank für Personenzertifikate auf den Erlaubnistatbestand Einwilligung stützen zu können, müsste **jede zertifizierte Person** als betroffene Person in die Verarbeitung

[89] Art 6 Abs 1 lit b DSGVO; ErwGr 44 DSGVO.
[90] Art 7 Abs 4 DSGVO; *Schulz* in Gola, DS-GVO[2] Art 6 Rz 36.
[91] Art 7 Abs 2 DSGVO.
[92] *Ingold* in Sydow, Europäische Datenschutzgrundverordnung (2. Aufl., 2018) Art 7 Rz 24.
[93] Art 6 Abs 1 lit a DSGVO.
[94] Art 4 Nr 11 DSGVO.

ihrer personenbezogenen Daten in Rahmen dieser Verarbeitungstätigkeit (vlg. oben Punkt 4.c)) **einwilligen**. Dies umfasst nicht nur die neu zertifizierten Personen, sondern auch die Inhaber der aktuellen und gültigen Zertifikate, somit alle Zertifikatsinhaber.

Die Einwilligung ist **gegenüber jedem einzelnen Verantwortlichen** (vgl. oben Punkt 4.d)i)) zu erklären.[95] Im Fall, dass eine neue Zertifizierungsstelle für Personen akkreditiert würde und diese dem Blockchain-System als schreibende Teilnehmerin beitreten würde, wäre sie grundsätzlich als zusätzliche (gemeinsame) Verantwortliche der Verarbeitung von personenbezogenen Daten in der zentralen Datenbank für Personenzertifikate anzusehen, daher hätte jede betroffene Person ihre Einwilligung gegenüber der neuen Verantwortlichen zu diesem späteren Zeitpunkt zu erteilen.[96] Das Einwilligungsverfahren wäre **allerdings dann nicht** zu „wiederholen", wenn die schreibenden Teilnehmer des Blockchain-Systems vor der Aufnahme der Verarbeitung der personenbezogenen Daten den Verantwortlichen identifiziert hätten und die neu akkreditierte Zertifizierungsstelle dieser Vereinbarung beitreten würde (vgl. oben Punkt 4.d)i) am Ende).

Ferner ist zu beachten, dass jede zertifizierte Person das Recht hat, ihre Einwilligung **jederzeit** zu **widerrufen**.[97] Ein Widerrufsgrund ist nicht erforderlich. Auf das Widerrufsrecht kann die betroffene Person datenschutzrechtlich auch **nicht verzichten**.[98]

Durch den Widerruf der Einwilligung wird zwar die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt („Wirkung ex nunc"), jedoch bleibt der bisherige Datenbestand dem Verantwortlichen nicht erhalten. Vielmehr greift insoweit regelmäßig die **Löschpflicht gemäß Art 17 DSGVO** (vgl. unten Punkt 4.f)iv)).[99]

Laut *Artikel-29-Datenschutzgruppe* ist die Datenverarbeitung (oder deren auf die Einwilligung gestützter Teil) bei Widerruf der Einwilligung auch dann zu beenden, wenn die Verarbeitung auf einen anderen Erlaubnistatbestand gestützt werden könnte. Begründet wird diese Ansicht damit, dass *„es gegenüber Einzelpersonen ein in höchstem Maß missbräuchliches Verhalten wäre, ihnen zu sagen, dass die Daten auf der Grundlage der Einwilligung verarbeitet werden, wenn tatsächlich eine andere Rechtsgrundlage zugrunde gelegt wird"* also mit dem Grundsatz von Treu und Glauben sowie dem Transparenzgrundsatz. Nach dieser Ansicht kann *„der Verantwortliche nicht von der Einwilligung zu einer anderen Rechtsgrundlage wechseln"* („Rückgriffsverbot").[100] In der Literatur wird hingegen vertreten, dass die Einwilligung „sicherheitshalber" eingeholt und die Verarbeitung auf mehrere Rechtsgrundlagen parallel gestützt werden kann, wenn dem Grundsatz von Treu und Glauben genüge getan wird. Insbesondere ist

---

[95] *Schrey/Thalhofer*, Rechtliche Aspekte der Blockchain, NJW 2017, 1431 (1434).
[96] *Schrey/Thalhofer*, Rechtliche Aspekte der Blockchain, NJW 2017, 1431 (1434).
[97] Art 7 Abs 3 DSGVO.
[98] *Ingold* in Sydow, EU-DSGVO[2] Art 7 Rz 46; *Heckmann/Paschke* in Ehmann/Selmayr, DS-GVO[2] Art 7 Rz 93.
[99] *Ingold* in Sydow, EU-DSGVO[2] Art 7 Rz 48.
[100] *Artikel-29-Datenschutzgruppe*, Leitlinien in Bezug auf die Einwilligung gemäß Verordnung 2016/679 (zuletzt überarbeitet und angenommen am 10. April 2018), 27f: *„Es ist beispielsweise nicht gestattet, rückwirkend das berechtigte Interesse als Grundlage für die Rechtfertigung der Verarbeitung zu wählen, wenn Probleme mit der Gültigkeit der Einwilligung aufgetreten sind. Aufgrund der Verpflichtung, die Rechtsgrundlage, auf die sich der Verantwortliche stützt, zum Zeitpunkt der Erhebung der personenbezogenen Daten anzugeben, müssen Verantwortliche vor der Erhebung entschieden haben, welche Rechtsgrundlage anwendbar ist."*.

die betroffene Person in diesen Fällen über das Bestehen dieser weiteren Rechtsgrundlage sowie über die Tatsache, dass ein jederzeit möglicher Widerruf der Einwilligung nicht unbedingt zur Einstellung der Verarbeitung führen muss, zu informieren.[101] Bis diese Literaturmeinungen durch die Judikatur bestätigt werden, kann allerdings nicht ohne Weiteres von der Möglichkeit des Rückgriffs auf eine weitere Rechtsgrundlage bei Widerruf der Einwilligung ausgegangen werden.

Ist die Heranziehung einer der oben geschilderten gesetzlichen Erlaubnistatbestände möglich, sollte daher die Verarbeitung nicht „sicherheitshalber" auf die Einwilligung der betroffenen Personen gestützt werden. Darüber hinaus kann sich die Stützung der Datenverarbeitung auf den Erlaubnistatbestand Einwilligung wegen deren jederzeitigen Wiederrufbarkeit als unzulänglich herausstellen, weil es wohl praktisch nicht möglich wäre, sämtliche Personenzertifikate in einer Datenbank zusammenzufassen und somit deren Vollständigkeit zu gewährleisten.

f) Rechte der betroffenen Person

Die DSGVO regelt umfassend die Rechte der betroffenen Personen und präzisiert auch das Verfahren zur deren **Erfüllung durch den Verantwortlichen**. Der Verantwortliche ist verpflichtet, geeignete Maßnahmen zu treffen, um seinen Informationspflichten durch Übermittlung von Informationen in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache an die betroffenen Personen nachzukommen.[102] Ferner ist der Verantwortliche verpflichtet den betroffenen Personen die Ausübung ihrer Rechte zu erleichtern („**Erleichterungsgrundsatz**").[103]

Wird es bei dem im Rahmen des Pilotprojekts entwickelten Blockchain-System mehrere gemeinsam Verantwortliche geben, ist eine **Regelung** über die Aufteilung von Zuständigkeiten für die Wahrnehmung und über die Modalitäten der Erfüllung der verschiedenen Rechte der betroffenen Personen vorzusehen (vgl. zu den möglichen Regelungsinstrumenten oben Punkt 4.d)i)).[104] Hierbei ist zu beachten, dass die betroffene Person ihre Rechte **bei und gegenüber jedem einzelnen der Verantwortlichen geltend machen kann**, selbst wenn die Verantwortliche untereinander eine andere Verteilung von Aufgaben hinsichtlich der Erfüllung der Rechte der betroffenen Personen vereinbaren.[105] Die Verantwortlichen können beispielsweise vorsehen, dass (i) alle Anträge auf Erfüllung der Rechte der betroffenen Personen auf die Akkreditierung Austria (oder einen anderen Verantwortlichen) weitergeleitet werden und durch diese

[101] Unter anderem *Schulz* in Gola, DS-GVO[2] Art 6 Rz 11ff, *Heckmann/Paschke* in Ehmann/Selmayr, DS-GVO[2] Art 7 Rz 20; *Buchner/Kühling* in Kühling/Buchner, DS-GVO/BDSG[2] Art 7 Rz 17ff; *Kastelitz/Hötzendorfer/Tschohl* in Knyrim, DatKomm Art 6 DSGVO (Stand 1.10.2018, rdb.at) Rz 15ff mwN.
[102] Art 12 Abs 1 DSGVO.
[103] Art 12 Abs 2 DSGVO, ErwGr 59 Satz 1 DSGVO.
[104] Art 26 Abs 1 und 2 DSGVO.
[105] Art 26 Abs 3 DSGVO.

zu erfüllen sind oder (ii) dass die Anträge immer an den Verantwortlichen weitergeleitet werden, welcher der beantragenden betroffenen Person das Zertifikat ausgestellt hat, und dieser die ihm übermittelte Anträge selbst erfüllt.

Die Blockchain-Systeme stehen wegen der „Unveränderbarkeit" der in der Blockchain gespeicherten Daten in einem **Spannungsverhältnis mit der effektiven Erfüllung bestimmter Rechte der betroffenen Personen**, die die Veränderung oder Löschung eines in der Blockchain gespeicherten Datums voraussetzen.[106] Vor diesem Hintergrund stellt sich die Frage, wie die Datenschutzkonformität des im Rahmen des Pilotprojekts entwickelten Blockchain-Systems gewährleistet werden kann. Aus diesem Grund werden nachstehend die Möglichkeiten zur Erfüllung des Rechts auf Berichtigung, des Widerspruchsrechts und des Rechts auf Löschung näher untersucht.[107]

i) Rechte der betroffenen Person, die mit der Verwendung der Blockchain-Technologie vereinbar sind

Die Informationspflichten der Verantwortlichen[108], das Auskunftsrecht der betroffenen Personen und das Recht auf Datenübertragbarkeit sind mit den technischen Eigenschaften der Blockchain vereinbar. Der **Einsatz der Blockchain** zur Verarbeitung von personenbezogenen Daten in der zentralen Datenbank für Personenzertifikate **führt zu keinen Besonderheiten bei Erfüllung** dieser Rechte.[109]

ii) Recht auf Berichtigung

Die verarbeiteten personenbezogenen Daten müssen sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein. Daher sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden („**Grundsatz der Richtigkeit**").[110] Dazu sollen alle vertretbaren Schritte unternommen werden.[111] Das Recht auf Richtigstellung unrichtiger Daten – wie auch das Recht auf Löschung unzulässigerweise verarbeiteter Daten – ist auch verfassungsrechtlich verankert.[112]

---

[106] *CNIL*, Blockchain, 8.
[107] *CNIL*, Blockchain, 8.
[108] „Aktive Transparenz" auf deren Erfüllung die betroffene Person einen Anspruch hat, vlg. etwa *Franck* in Gola, DS-GVO[2] Art 13 Rz 56ff, Art 14 Rz 36.
[109] *CNIL*, Blockchain, 8: *„Rights that are entirely compatible with a blockchain"*.
[110] Art 5 Abs 1 lit d DSGVO.
[111] ErwGr 39 Satz 11 DSGVO.
[112] § 1 Abs 3 Z 2 DSG.

(1) Berichtigung und Vervollständigung

Die betroffene Person hat *"das Recht, von dem Verantwortlichen unverzüglich die Berichtigung sie betreffender unrichtiger personenbezogener Daten zu verlangen"* (Recht auf Berichtigung ieS).[113] Ferner hat die betroffene Person unter Berücksichtigung der Zwecke der Verarbeitung *„das Recht, die Vervollständigung unvollständiger personenbezogener Daten – auch mittels einer ergänzenden Erklärung – zu verlangen"* (Recht auf Vervollständigung).[114]

Werden in der zentralen Datenbank für Personenzertifikate personenbezogene Daten verarbeitet, welche nicht mit der Realität übereinstimmen, wird beispielsweise eine falsches Zertifizierungsprogramm oder ein unzutreffender Geltungsbereich der Zertifizierung gespeichert oder fehlt schlicht ein Datum, etwa das Ablaufdatum der Zertifizierung, ist der unrichtige Datensatz zu berichtigen.[115]

Die DSGVO sieht eine Vervollständigung auch mittels **ergänzender Erklärung** (*supplementary statement*) vor, setzt aber voraus, dass die Vervollständigung der Daten selbst unmöglich oder untunlich ist.[116] Die ergänzende Erklärung dient dabei als eine Art Gegendarstellung, durch welche die für die Zwecke der Verarbeitung benötigte **Inhaltswahrheit erreicht** wird.[117] Da auch die Berichtigung ieS den gleichen Zweck, nämlich die Inhaltswahrheit, verfolgt, ist anzunehmen, dass ein ergänzende Erklärung auch zur Berichtigung von unrichtigen personenbezogen Daten herangezogen werden darf, sofern die Berichtigung der Daten selbst unmöglich oder untunlich ist. Ferner ist unseres Erachtens unbedeutend aus welchem Grund die Vervollständigung und/oder Berichtigung der Daten selbst unmöglich oder untunlich sind, daher ist auch bei einer Unmöglichkeit bzw. Untunlichkeit aus technischen Gründen die Berichtigung und Vervollständigung durch ergänzende Erklärung zulässig.

Im Hinblick auf die „Unveränderbarkeit" der Blockchain ist davon auszugehen, dass in der zentralen Datenbank für Personenzertifikate sowohl die Berichtigung ieS als auch die Vervollständigung der gespeicherten Daten selbst unmöglich bzw. untunlich sein werden, daher kann die Inhaltswahrheit der Daten durch eine ergänzende Erklärung hergestellt werden.

Bei einer Blockchain kommen sog. **„Reverse transactions"** als ergänzende Erklärungen in Frage. Da der Inhalt der Blöcke, die die unrichtigen personenbezogenen Daten beinhalten, grundsätzlich nicht geändert werden kann (vgl. aber dazu unten 4.f)iv)(1)(c)), ist eine (fiktive) Eintragung in die Blockchain vorzunehmen, die den inhaltlich korrekten Status, die Inhalts-

---

[113] Art 16 Satz 1 DSGVO.
[114] Art 16 Satz 2 DSGVO.
[115] *Kamann/Braun* in Ehmann/Selmayr, DS-GVO Art 16 Rz 16; *Haidinger* in Knyrim, DatKomm Art 17 DSGVO (Stand 1.10.2018, rdb.at) Rz 22.
[116] *Haidinger* in Knyrim, DatKomm Art 17 DSGVO (Stand 1.10.2018, rdb.at) Rz 36; *Feiler/Forgó*, EU-DSGVO Art 16 Rz 2.
[117] *Kamann/Braun* in Ehmann/Selmayr, DS-GVO Art 16 Rz 42.

wahrheit, herstellt. Der **neue Block** mit inhaltlich richtigen personenbezogenen Daten **berichtigt** oder vervollständigt **den alten Block** mit unrichtigen Daten und wird anschließend anstatt diesen beauskunftet.[118]

Die Berichtigung der unrichtigen Daten hat unverzüglich, somit **ohne schuldhaftes Zögern**, zu erfolgen. Diese Anforderung wird durch eine Monatsfrist, welche bei komplexeren Fällen auf drei Monate verlängert werden darf, konkretisiert.[119] Die ergänzende Erklärung sollte somit unverzüglich nach Erhalt des Berichtigungsantrags vorgenommen werden.

Die Berichtigung durch eine ergänzende Erklärung lässt den **alten „berichtigten" Block** und die darin enthaltenen personenbezogenen Daten intakt. Die Verarbeitung dieser personenbezogenen Daten ist für die Zwecke der zentralen Datenbank für Personenzertifikate (vgl. oben Punkt 4.c)i)) allerdings nicht mehr notwendig, daher ist der alte Block (ohne schuldhaftes Zögern) **zu löschen**. Kann die Löschung – sollte diese in der konkreten Blockchain überhaupt technisch möglich sein – nicht umgehend erfolgen, ist bis dahin die Verarbeitung von den in alten Blöcken enthaltenen personenbezogenen Daten einzuschränken (dies kann etwa durch Sperrung des Zugriffs auf einen gewissen Datensatz erfolgen[120]; vgl. zur Löschung gleich unten Punkt 4.f)iv)).[121]

(2) Mitteilungspflicht

Der Verantwortliche ist verpflichtet, allen Empfängern, denen personenbezogene Daten offengelegt wurden, jede Berichtigung oder Löschung der personenbezogenen Daten sowie eine Einschränkung der Verarbeitung („**korrigierende Veränderung**") mitzuteilen, *„es sei denn, dies erweist sich als unmöglich oder ist mit einem unverhältnismäßigen Aufwand verbunden"* („Nachberichtspflicht").[122] Die Empfänger sind natürliche oder juristische Personen, Behörden, Einrichtungen oder andere Stellen, denen personenbezogene Daten offengelegt werden, *„unabhängig davon, ob es sich bei ihnen um einen Dritten handelt oder nicht"*.[123] Die Empfänger sind somit nicht nur die (anderen) Verantwortlichen und Auftragsverarbeiter, sondern auch die interessierten Unternehmen und Personen, welche die Auskünfte über Zertifikate aus der Datenbank erhalten haben.

Diese Nachberichtspflicht besteht nicht, wenn deren Erfüllung sich als (i) unmöglich, etwa wenn der Empfänger nicht mehr existent oder unbekannt ist, was bei Veröffentlichungen der Fall sein kann, oder (ii) als mit **unverhältnismäßigem Aufwand** verbunden erweist.[124] Ob ein

---

[118] *CNIL*, Blockchain, 9; *Finck*, Blockchains and Data Protection in the European Union, 22; vgl. auch *Schrey/Thalhofer*, Rechtliche Aspekte der Blockchain, NJW 2017, 1431 (1435) wohl aA mit der Begründung, dass *„die Transaktion selbst […] jedoch erhalten [bleibe]"*.

[119] *Reif* in Gola, DS-GVO[2] Art 16 Rz 18; Art 12 Abs 3 DSGVO.

[120] ErwGr 67 Satz 1 DSGVO.

[121] *CNIL*, Blockchain, 9.

[122] Art 19 Satz 1 DSGVO.

[123] Art 4 Nr 9 Satz 1 DSGVO.

[124] *Gola* in Gola, DS-GVO[2] Art 19 Rz 7, 10; *Haidinger* in Knyrim, DatKomm Art 19 DSGVO (Stand 1.10.2018, rdb.at) Rz 16.

solcher unverhältnismäßiger Aufwand vorliegt, ist im Einzelfall unter Abwägung der zu investierenden Menge an Zeit und Geld des Verantwortlichen mit den berechtigten Interessen der betroffenen Person festzustellen.[125] Daher ist auch bei der Weitergabe von Daten an bestimmte Empfänger möglich, dass für die Feststellung ihrer Identität ein unverhältnismäßiger Aufwand betrieben werden müsste.[126] Häufiger wird diese Ausnahme jedoch anwendbar sein, wenn die Kommunikationsdaten der Empfänger erst erhoben werden müssten, etwa weil deren Kreis unbestimmt ist.[127]

Im Rahmen der im Pilotprojekt entwickelten zentralen Datenbank für Personenzertifikate werden personenbezogene Daten zum Abruf bereitgestellt. Um sämtliche Empfänger dieser Daten von der Korrektur zu benachrichtigen, müsste ein automatisiertes Nachmeldeverfahren entwickelt werden. Die Programmierung eines automatischen Nachmeldeverfahrens in einem Blockchain-System wäre unseres Erachtens, selbst wenn diese technisch möglich sein sollte, allerdings mit unverhältnismäßigen Aufwand verbunden, daher entfällt die Nachberichtspflicht und die Berichtigung durch die **Korrektur im Datenbestand** des Verantwortlichen, **aus dem die Daten zu Beauskunftung abgerufen werden, ist ausreichend** (vgl. oben Punkt 4.f)ii)(1)).[128]

Der Verantwortliche ist ferner grundsätzlich verpflichtet, die betroffene Person auf deren Antrag über *„diese“* Empfänger zu unterrichten („Folgeunterrichtung“).[129] Da bei der zentralen Datenbank für Personenzertifikate die aktive Nachberichtigung der Empfänger wegen deren Unverhältnismäßigkeit entfällt, sind diese der betroffenen Personen jedoch nicht mitzuteilen.[130]

iii) Widerspruchsrecht

Die betroffene Person hat *„das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung sie betreffender personenbezogener Daten, die aufgrund von Artikel 6 Absatz 1 Buchstaben e oder f erfolgt, Widerspruch einzulegen“*.[131] Soweit die Verarbeitung von personenbezogenen Daten in der zentralen Datenbank (unter anderem) auf die berechtigten Interessen des Verantwortlichen oder eines Dritten gestützt wird (vgl. oben Punkt **Fehler! Verweisquelle konnte nicht gefunden werden.**), muss die betroffene Per-

[125] *Gola* in Gola, DS-GVO[2] Art 19 Rz 11; *Haidinger* in Knyrim, DatKomm Art 19 DSGVO (Stand 1.10.2018, rdb.at) Rz 16.
[126] *Haidinger* in Knyrim, DatKomm Art 19 DSGVO (Stand 1.10.2018, rdb.at) Rz 16.
[127] *Haidinger* in Knyrim, DatKomm Art 19 DSGVO (Stand 1.10.2018, rdb.at) Rz 16.
[128] Dies ist in der Literatur strittig, vlg. *Herbst* in Kühling/Buchner, DS-GVO/BDSG[2] Art 19 Rz 12, wonach sich das nicht pauschal beantworten lässt, sonder es vielmehr auf die Häufigkeit des Abrufens ankommt (mit weiteren Nachweisen der deutschen Literatur dafür und dagegen); für Unverhältnismäßigkeit iSd Art 19 DSGVO im Zusammenhang mit Blockchain auch *Finck*, Blockchains and Data Protection in the European Union, 22.
[129] Art 19 Satz 2 DSGVO.
[130] *Gola* in Gola, DS-GVO[2] Art 19 Rz 15; *Kamann/Braun* in Ehmann/Selmayr, DS-GVO Art 19 Rz 28.
[131] Art 21 Abs 1 Satz 1 DSGVO.

son spätestens zum Zeitpunkt der ersten Kommunikation mit ihr ausdrücklich auf ihr (allgemeines) Widerspruchsrecht hingewiesen werden.[132] Wird die Datenverarbeitung nicht nur auf die berechtigten Interessen des Verantwortlichen oder eines Dritten, sondern auf **mehrere Rechtsgrundlagen parallel** gestützt, ist die betroffene Person dem Grundsatz von Treu und Glauben entsprechend über das Bestehen dieser weiteren Rechtsgrundlage, im gegenständlichen Fall der (Informationspflicht nach) ISO 17024, sowie über die Tatsache, dass selbst ein statthafter Widerspruch nicht unbedingt zur Einstellung der Verarbeitung führen muss, zu informieren (vgl. oben Punkt 4.e)i)).

Das Widerspruchsrecht zielt darauf ab, eine rechtmäßige Datenverarbeitung ausnahmsweise unzulässig zu machen, und knüpft daher an das Vorliegen einer **besonderen Situation** der betroffenen Person an.[133] Diese kann sich sowohl aus veränderten Umständen in der Person des Betroffenen als auch durch eine sich nachträglich verändernde Eingriffsqualität oder eine neue Gefahrenquelle ergeben, was jeweils im Einzelfall zu prüfen ist.[134] Bei der Beurteilung ist ein strenger Maßstab anzulegen, weshalb in der Regel nur Situationen, in denen durch eine fortgesetzte Datenverarbeitung – nunmehr – eine Gefahr für Leib und Leben, das Eigentum oder für eine in ihrer Bedeutung vergleichbare (absolute) Rechtsposition der betroffenen Person darstellt, erfasst werden.[135]

Es kann nicht (im Voraus) ausgeschlossen werden, dass eine derartige Situation hinsichtlich einer der zertifizierten Personen eintritt, deren personenbezogene (Zertifikats-)Daten in der zentralen Datenbank für Personenzertifikate gespeichert werden. Im Fall eines berechtigten Widerspruchs darf der Verantwortliche die personenbezogenen Daten nicht mehr verarbeiten. In diesem Fall sind auch die Voraussetzungen für einen Löschungsanspruch gegeben, den der Verantwortliche selbständig – ohne zusätzlichen Antrag der betroffenen Person – zu erfüllen hat (**Löschgrund**[136], vgl. zur Löschung unten Punkt 4.f)iv)).[137]

Ein (an sich statthafter) Widerspruch führt allerdings dann nicht zur Beendigung der Datenverarbeitung, wenn der Verantwortliche *„zwingende schutzwürdige Gründe für die Verarbeitung nachweisen [kann], die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen, oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen“*.[138]

Selbst wenn keine zwingenden schutzwürdigen Gründe für die Fortsetzung der Datenverarbeitung vorliegen und die Daten nicht zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigt werden, kann jedoch der Löschungsanspruch ausgeschlossen werden, wenn *„vorrangige berechtigte Gründe für die Verarbeitung“*, etwa die technische

[132] Art 21 Abs 4 DSGVO.
[133] *Schulz* in Gola, DS-GVO[2] Art 21 Rz 8.
[134] *Schulz* in Gola, DS-GVO[2] Art 21 Rz 9.
[135] *Schulz* in Gola, DS-GVO[2] Art 21 Rz 9.
[136] Art 17 Abs 1 lit c DSGVO.
[137] *Haidinger* in Knyrim, DatKomm Art 21 DSGVO (Stand 1.10.2018, rdb.at) Rz 38.
[138] Art 21 Abs 1 Satz 2 DSGVO.

Weiterentwicklung der Software, vorliegen.[139] Diese stellen gegenüber dem Begriff des zwingenden schutzwürdigen Grundes ein Minus dar.[140] Es sind daher Fallgestaltungen denkbar, in denen die weitere Datenverarbeitung zwar aufgrund des Widerspruchs ausgeschlossen, der Verantwortliche aber nicht zur Löschung der Daten verpflichtet ist.[141]

Aufgrund der die Zertifizierungsstellen treffenden Pflicht, die Informationen über aktuelle und gültige Personenzertifikate öffentlich zur Verfügung zu stellen (vgl. oben Punkt 4.a)ii)(2)), werden in der Regel zwingende schutzwürdige Gründe oder zumindest **vorrangige berechtigte Gründen für die weitere Datenverarbeitung** vorliegen, wenn eine zertifizierte Person der Verarbeitung ihrer personenbezogenen (Zertifikats-)Daten, welche sich auf ein aktuelles und gültiges Personenzertifikat beziehen, widersprechen wird. Sollten im Einzelfall doch keine vorrangigen berechtigten Gründe vorliegen, wäre die Verarbeitung der personenbezogenen Daten, welcher widersprochen wurde, einzustellen und diese Daten aus der zentralen Datenbank für Personenzertifikate zu löschen (vgl. gleich unten Punkt 4.f)iv)).

iv) Recht auf Löschung

Die verarbeiteten personenbezogenen Daten müssen in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist („**Grundsatz der Speicherbegrenzung**“).[142] Die Verantwortlichen sollten alle vertretbaren Schritte unternehmen, um die personenbezogenen Daten zu löschen und nicht mehr zu verarbeiten, wenn ihre Speicherung gegen die DSGVO oder gegen das Unionsrecht oder das Recht der Mitgliedstaaten, dem der Verantwortliche unterliegt, verstößt.[143]

(1) Löschrechte

(a) Löschanspruch und Löschpflicht

Die betroffene Person hat gegenüber dem Verantwortlichen einen Anspruch auf unverzügliche Löschung der sie betreffenden personenbezogenen Daten („**Löschanspruch**“), wenn (lit a) diese für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig sind („Zweckerfüllung“), (lit b) sie ihre Einwilligung widerruft und es fehlt an einer anderweitigen Rechtsgrundlage für die Verarbeitung („Widerruf der Einwilligung“), (lit c) sie einen Widerspruch gegen die Verarbeitung einlegt, (lit d) die personenbezogenen Daten

[139] Art 17 Abs 1 lit c DSGVO.
[140] *Nolte/Werkmeister* in Gola, DS-GVO[2] Art 17 Rz 18; aA *Herbst* in Kühling/Buchner, DS-GVO/BDSG[2] Art 17 Rz 26, welcher den Ausdrücken trotz unterschiedlichen Wortlauts die gleiche Bedeutung beimisst.
[141] *Nolte/Werkmeister* in Gola, DS-GVO[2] Art 17 Rz 19.
[142] Art 5 Abs 1 lit e DSGVO.
[143] ErwGr 39 Satz 11 iVm ErwGr 65 Satz 1 und 2 DSGVO.

unrechtmäßig verarbeitet wurden, (lit e) die Löschung der personenbezogenen Daten zur Erfüllung einer rechtlichen Verpflichtung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten erforderlich ist, dem der Verantwortliche unterliegt („Öffnungsklausel"), oder (lit f) die personenbezogenen Daten in Bezug auf angebotene Dienste der Informationsgesellschaft bei Minderjährigen erhoben wurden („**Löschgründe**").[144] Den Verantwortlichen trifft in diesen Fällen eine eigenständige von Geltendmachung des Löschanspruchs unabhängige **Löschpflicht**.[145]

Bei der Verarbeitung von personenbezogenen Daten in der zentralen Datenbank für Personenzertifikate können gleich mehrere dieser Tatbestände erfüllt werden. Am häufigsten wird eine Löschpflicht entstehen, wenn die Gültigkeitsdauer eines Zertifikats abläuft, ohne dass dieses verlängert bzw. erneuert wird. In diesem Fall wird die Verarbeitung der Zertifikatsdaten zur Erteilung von Auskünften über (aktuelle und gültige) Personenzertifikate an die Öffentlichkeit (vgl. oben Punkt 4.c)i)) nicht mehr notwendig sein, daher sind diese zu löschen.

(b) Begriff Löschung iSd DSGVO

Der Begriff der Löschung wird in der DSGVO nicht definiert. Er umfasst jedwede Art der **Unkenntlichmachung**, nicht nur endgültige physische Vernichtung. Dem Verantwortlichen steht hinsichtlich der Mittel – sohin der vorgenommenen Art und Weise der Löschung ein – Auswahlermessen zu.[146] Wesentlich ist, dass die Daten für den Verantwortlichen **unlesbar geworden** sind oder **diesem nicht mehr zur Verfügung stehen** und, dass weder der Verantwortliche selbst, noch ein Dritter ohne unverhältnismäßigen Aufwand einen Personenbezug wiederherstellen kann.[147] **Völlige Irreversibilität ist jedoch** – unabhängig vom verwendeten Mittel zur Löschung – **nicht notwendig**.[148]

Im Ergebnis verlangt die DSGVO somit eine **wirkungsorientierte Löschung** und nicht die tatsächliche Vernichtung der Daten.

---

[144] Art 17 Abs 1 DSGVO.

[145] Art 17 Abs 1 UAbs 1 DSGVO; *Haidinger* in Knyrim, DatKomm Art 17 DSGVO (Stand 1.10.2018, rdb.at) Rz 17.

[146] DSB-D123.270/0009-DSB/2018 vom 5.12.2018 mwN; *Kamann/Braun* in Ehmann/Selmayr, DS-GVO Art 17 Rz 36.

[147] DSB-D123.270/0009-DSB/2018 vom 5.12.2018 mwN; *Nolte/Werkmeister* in Gola, DS-GVO[2] Art 17 Rz 10; *Kamann/Braun* in Ehmann/Selmayr, DS-GVO Art 17 Rz 32; *Haidinger* in Knyrim, DatKomm Art 17 DSGVO (Stand 1.10.2018, rdb.at) Rz 63; *Finck*, Blockchains and Data Protection in the European Union, 25.

[148] DSB-D123.270/0009-DSB/2018 vom 5.12.2018mwN; *Kamann/Braun* in Ehmann/Selmayr, DS-GVO Art 17 Rz 33; *Haidinger* in Knyrim, DatKomm Art 17 DSGVO (Stand 1.10.2018, rdb.at) Rz 63; *Finck*, Blockchains and Data Protection in the European Union, 25.

(c) (Technische) Umsetzbarkeit in der Blockchain

Eine unmittelbare Anwendung des Rechts auf Löschung ist bei Verwendung einer **Blockchain** – wie im Rahmen des Pilotprojekts – wegen ihrer „**Unveränderbarkeit**“ nicht möglich.[149]

Mit Unveränderbarkeit wird idR gemeint, dass eine *unbemerkte* rückwirkende Veränderung der Informationen, die in der Blockchain gespeichert sind, unmöglich erscheint.[150] Wenn die Daten innerhalb einer Blockchain gespeichert werden, werden diese (in der Regel) nämlich über kryptographische Hashwerte miteinander verkettet. Verändert man einen Datensatz innerhalb von einem Block stimmen die kryptographischen Hashwerte nicht mehr und die gesamte Blockchain ist inkonsistent, was sich sofort feststellen lässt, weshalb diese Version der Blockchain im Blockchain-System durch andere Blockchain-Knoten (*Nodes*) nicht akzeptiert wird.[151]

Die *CNIL* schlägt einige Wege vor, wie das Recht auf Löschung in der Blockchain umgesetzt werden könnte. Die Daten könnten in der Blockchain als Commitments[152], Hash generiert durch eine Keyed-hash Funktion oder als Chiffretext generiert durch einen dem Stand der Technik entsprechenden Algorithmus und Schlüssel (*key*) gespeichert werden, was diese praktisch unzugänglich macht und sich daher näher in die Richtung der wirkungsorientierten Löschung bewegt.[153] Wenn die Identifikationselemente eines Commitments (*witness*)[154] oder der geheime Schlüssel der Keyed-hash Funktion gelöscht werden, füht dies zwar nicht zur physischen Löschung der Daten aus der Blockchain, sondern diese existieren dort weiter, werden jedoch für alle, insbesondere auch den (bis dahin) Verantwortlichen, unzugänglich (*„inaccessible“*). Diese Verfahren können auch formalisiert werden, und die betroffenen Personen können über deren Ablauf und Folgen (vorab) informiert werden. Es sollte daher – im Einzelfall – **die Äquivalenz eines Verfahren mit der wirkungsorientierten Löschung iSd DSGVO beurteilt werden**.[155] Um diesen Anforderungen zu entsprechen, müssen die personenbezogenen Daten, die in der Blockchain gespeichert sind, unlesbar bzw. unverfügbar und somit für alle unkenntlich gemacht werden. **Eine technische Implementierung des Rechts auf Löschung in der Blockchain ist daher – aus Perspektive des Datenschutzrechts – möglich**.

---

[149] *Finck*, Blockchains and Data Protection in the European Union, 23f.

[150] *BaFin*, Blockchain-Technologie, https://www.bafin.de/DE/Aufsicht/FinTech/Blockchain/blockchain_node.html; Gabler Wirtschaftslexikon, Blockchain, https://wirtschaftslexikon.gabler.de/definition/blockchain-54161/version-277215.

[151] *Ploom*, Blockchains - wichtige Fragen aus IT-Sicht in *Burgwinkel* (Hrsg.), Blockchain Technology: Einführung für Business- und IT Manager (2016), 1, 130f, https://www.researchgate.net/publication/311856912_Blockchains_-_wichtige_Fragen_aus_IT-Sicht_Einfuhrung_fur_Business-_und_IT_Manager.

[152] *CNIL*, Blockchain, 6 FN 1: *„A “commitment” is a cryptographic mechanism that allows one to “freeze” data in such a way that it is both possible - with additional information - to prove what has been frozen and impossible to find or recognise such data by using this sole “commit”“*.

[153] *CNIL*, Blockchain, 8.

[154] *CNIL*, Blockchain, 8 FN 2 “*When a commitment scheme is perfectly hiding, deleting the **witness** (i.e. the element that allows to verify that a given value is committed in a given commit) and the value committed is sufficient to render the commitment anonymous in such a way that it can no longer be considered personal data”*.

[155] *CNIL*, Blockchain, 8f.

Bei **zulassungsbeschränkten Blockchain-Systemen** sind mehrere technische und organisatorische Möglichkeiten, welche eine Änderung der in der Blockchain gespeicherten Daten (*on chain*) ermöglichen denkbar. Diese sind nachstehend darauf zu untersuchen, ob sie geeignet sind das Rechts auf Löschung umzusetzen.

Vergleichbar mit einem "51%-Attack" wäre in einer zulassungsbeschränkten Blockchain möglich, dass die (schreibenden) Teilnehmer aufgrund eines Konsensmechanismus ein **Rollback** vereinbaren. Dadurch würde jedoch nicht nur der Block mit den zu löschenden Daten geändert, sondern auch alle diesem in der Blockchain folgende Blöcke gelöscht, welche in der Folge wieder in die Blockchain einzutragen wären.[156] Fraglich ist daher, ob die Umsetzung dieser Option nicht mit unverhältnismäßigem Aufwand verbunden wäre.

Des Weiteren können in einem Blockchain-System durch **Pruning**[157] obsolete Daten aus älteren Blöcken entfernt werden, wenn diese für die Weiterbildung der Blockchain nicht mehr benötigt werden.[158] Ähnliche Wirkung kann erreicht werden, wenn eine Blockchain vom vornherein auf die nachträgliche Veränderbarkeit ausgelegt ist und ein **Chameleon Hash** verwendet wird. Dieser ist wandlungsfähig und lässt auch Änderung an bereits in der Kette eingebetteten Blöcken zu.[159] **Beide** diese Verfahren sind geeignet, eine Unkenntlichmachung der personenbezogenen Daten herbeizuführen, welche in der Blockchain (*on chain*) gespeichert sind, die den Anforderungen der **wirkungsorientierten Löschung iSd DSGVO** gerecht wird, **setzen allerdings den Einsatz einer zentralen Instanz oder eines anderen Mechanismus voraus, die/der die Vornahme der Löschungen in der Blockchain gewährleistet**.[160] Bei der Blockchain, auf welcher die zentralen Datenbank für Personenzertifikate basieren wird, können solche Lösungen – nicht zuletzt aufgrund der unterschiedlichen Rollen der Teilnehmer des Blockchain-Systems – vorgesehen werden (vgl. dazu gleich unten Punkt 4.f)iv)(1)(d)).

Eine weitere Möglichkeit bietet ferner die (nachträgliche) **Anonymisierung durch Löschung der Zuordnungsdaten**. Zu diesem Zweck können (i) anstelle der Daten, die in der Blockchain selbst gespeichert werden, die außerhalb der Blockchain gespeicherten Zuordnungsdaten öffentlicher Schlüssel gelöscht werden. Alternativ kann (ii) die Zuordnung gekappt werden.[161]

---

[156] *Greenspan*, The Blockchain Immutability Myth (4.5.2017), abrufbar unter https://www.multichain.com/blog/2017/05/blockchain-immutability-myth/, *„To solve this problem without chameleon hashes, nodes would have to rewrite the early block without the problematic transaction, calculate the block's new hash, then change the hash embedded in the next block to match. But this would also affect the next block's own hash, which must be recalculated and updated in the subsequent block, and so on all the way along the chain."*

[157] Zum Konzept des Prunings und seiner Verwendung als Mittel zur – hier automatischen – Löschung von ungenützten älteren Daten aus technischen Gründen vgl. etwa *Buterin*, State Tree Pruning (26.6.2015), https://blog.ethereum.org/2015/06/26/state-tree-pruning/.

[158] *Martini/Weinzierl*, Die Blockchain-Technologie und das Recht auf Vergessenwerden, NVwZ 2017, 1251 (1257); *Finck*, Blockchains and Data Protection in the European Union, 24.

[159] *Martini/Weinzierl*, Die Blockchain-Technologie und das Recht auf Vergessenwerden, NVwZ 2017, 1251 (1256); *Finck*, Blockchains and Data Protection in the European Union, 24.

[160] *Martini/Weinzierl*, Die Blockchain-Technologie und das Recht auf Vergessenwerden, NVwZ 2017, 1251 (1256f); *Finck*, Blockchains and Data Protection in the European Union, 24.

[161] *Martini/Weinzierl*, Die Blockchain-Technologie und das Recht auf Vergessenwerden, NVwZ 2017, 1251 (1256); *Schor,* On Zero-Knowledge Proofs in Blockchains, https://medium.com/@argongroup/on-zero-knowledge-proofs-in-blockchains-14c48cfd1dd1**.**

Diese Maßnahmen kommen allerdings bei der zentralen Datenbank für Personenzertifikate nur in Betracht, wenn sie die Voraussetzungen einer wirkungsorientierten Löschung erfüllen. Dies ist der Fall, wenn sichergestellt wird, dass durch die Löschung der Zuordnungsdaten zu den Identifikationsnummern der Teilnehmer und den Zertifikatnummern, welche in verschiedenen Ästen (*streams*) der Blockchain als öffentliche Schlüssel dienen, der Personenbezug der Daten sowohl für den Verantwortlichen als auch für andere Personen unkenntlich gemacht wird.

Zusätzlich zu den oben dargestellten (zielführenden) Verfahren bestehen weitere technische Möglichkeiten, die als Mittel zur Umsetzung des Rechts auf Löschung vorgeschlagen wurden, welche aber dem Zweck des im Rahmen des Pilotprojekts entwickelten Blockchain-Systems zuwiderlaufen und für die Verwendung in der zentralen Datenbank für Personenzertifikate nicht geeignet sind (aber vollständigkeitshalber auch kurz beleuchtet werden sollten). Eine Änderung der Blockchain kann etwa auch durch einen **Hard-Fork** herbeigeführt werden. Diese sind einerseits sehr aufwändig und machen nur beim zuletzt geschaffenen Block Sinn, weil alle dem Geänderten folgende Blöcke ebenso geändert werden, und sie wieder zu prozessieren wären. Hard-Forks sind daher keine geeignete Mittel zur Umsetzung des Rechts auf Löschung.[162] Wohl ungeeignet ist auch der Einsatz von **Zero-knowledge-proof (ZKP)-Verfahren**, durch welche die Identifizierbarkeit der handelnden Akteure ausgeschlossen wird, die aber nicht zur Löschung oder Anonymisierung der Daten, welche in der Blockchain selbst gespeichert sind, herangezogen werden können.[163]

Kann im Pilotprojekt keine der oben geschilderten technischen Maßnahmen, welche zur wirkungsorientierten Löschung der in der Blockchain gespeicherten personenbezogenen Daten führen, umgesetzt werden, könnte in gewissen Abständen die alte Blockchain gelöscht und eine neue mit aktuellen und bereinigten (sowie allenfalls berichtigten) Zertifikatsdaten geschafft werden („**Neuauflage der Blockchain**"). Durch die Neuauflage der Blockchain stehen die zu löschende Daten dem Verantwortlichen nicht mehr zu Verfügung und sind damit für ihn unkenntlich gemacht worden und daher gelöscht (vgl. oben Punkt 4.f)iv)(1)(b)).

„*Kann die Berichtigung oder Löschung von automationsunterstützt verarbeiteten personenbezogenen Daten nicht unverzüglich erfolgen, weil diese **aus wirtschaftlichen oder technischen Gründen nur zu bestimmten Zeitpunkten** vorgenommen werden kann*", so kann diese aufgeschoben werden, sofern die Datenverarbeitung bis dahin mit der Wirkung nach Art 18 Abs 2 DSGVO eingeschränkt wird.[164] Die (Berichtigung oder) Löschung der personenbezogenen Daten kann anschließend etwa bei Datenbankreorganisation, Stammdatenänderungslauf oder routinemäßigem Überspielen von Datenträgern mit Sicherungskopien erfolgen.[165] Die Neuauflage der Blockchain wird sowohl wegen technischer Komplexität als auch wegen Kosten-

[162] *Finck*, Blockchains and Data Protection in the European Union, 25; *Bechtolf/Vogt*, Datenschutz in der Blockchain – Eine Frage der Technik, ZD 2018, 66 (70).
[163] *Martini/Weinzierl*, Die Blockchain-Technologie und das Recht auf Vergessenwerden, NVwZ 2017, 1251 (1256).
[164] § 4 Abs 2 Datenschutzgesetz in der Form des Datenschutz-Deregulierungs-Gesetzes 2018, BGBl. I Nr. 24/2018 („**DSG**").
[165] *Haidinger* in Knyrim, DatKomm Art 17 DSGVO (Stand 1.10.2018, rdb.at) Rz 20.

aufwandes nur in gewissen Abständen möglich sein. Die Neuauflage **einmal jährlich** ist unseres Erachtens vertretbar und in einer Abwägung des Löschungsinteresses der betroffenen Person und der technischen und wirtschaftlichen Möglichkeiten der Teilnehmer des Blockchain-Systems der zentralen Datenbank für Personenzertifikate angemessen.

Bis zur Neuauflage der Blockchain sind die Löschbegehren der zertifizierten Personen zu sammeln und – falls diese als berechtigt angesehen werden – die Verarbeitung der zu löschenden Zertifikatsdaten einzuschränken. Die **Einschränkung der Verarbeitung** kann darin bestehen, dass die zu löschenden personenbezogenen Daten für Nutzer der zentralen Datenbank für Personenzertifikate gesperrt werden.[166] Anschließend dürfen diese Zertifikatsdaten grundsätzlich nur noch gespeichert und in keiner anderen Wiese weiterverarbeitet, vor allem nicht beauskunftet, werden.[167]

(d) Durchsetzbarkeit der Löschung im Blockchain-System

Um das Recht auf Löschung in einem Blockchain-System durchsetzen zu können, ist eine **Beschränkung von Schreib- und Leseberechtigungen** vorzusehen.[168] Dies kann bei einer zulassungsbeschränkten Blockchain dadurch erreicht werden, dass der Kreis der Blockchain-Knoten (*Nodes*) eingeschränkt wird, indem die Anzahl der Teilnehmer möglichst gering gehalten wird. Die Schreibbefugnis ist daher den Teilnehmern nur aufgrund deren Rolle in der Personen-Zertifizierung (Akkreditierungsstelle und Zertifizierungsstellen) einzuräumen (vgl. oben Punkt 4.c)ii)). Ferner ist die Anzahl der nicht-schreibenden Teilnehmern, die „einfache“ Betreiber von Blockchain-Knoten sind, zu beschränken (vgl. oben Punkt 4.d)ii). Wie oben dargestellt, besteht eine Pflicht der Zertifizierungsstellen die Informationen über aktuelle und gültige Personenzertifikate öffentlich zur Verfügung zu stellen (vgl. oben Punkt 4.a)ii)(2)). Eine Einschränkung der Leseberechtigung ist daher mit dem Zweck der zentralen Datenbank für Personenzertifikate unvereinbar (vgl. oben Punkt 4.c)i)). Die Implementierung einer öffentlich einsehbaren Blockchain lässt die Leseberechtigung uneingeschränkt. Eine Möglichkeit die Leseberechtigung (auf den ersten Blick) einzuschränken, ist (ii) der Einsatz von Serviceanbieter, die als Auskunftsstellen für die Öffentlichkeit und somit als eine Art „Gatekeeper“ des Blockchain-Systems dienen können. Allerdings wären auch diese verpflichtet auf Anfrage der interessierten Personen die relevanten Informationen über Personenzertifikate zu erteilen, daher würde auch der Einsatz von Serviceanbietern nicht zur effektiven Einschränkung der Leseberechtigung führen (vgl. auch oben Punkt 4.c)iii)).

Des Weiteren ist zu beachten, dass bei einer Blockchain die Löschung eines Datums eine gesonderte **Löschung bei jedem Blockchain-Knoten** voraussetzt[169] und auch bei einer zulassungsbeschränkten Blockchain, wie bei der im Rahmen des Pilotprojekts entwickelten, der

---

[166] ErwGr 67 Satz 1 DSGVO.
[167] Art 18 Abs 2 DSGVO; ErwGr 67 Satz 2 DSGVO.
[168] *Martini/Weinzierl*, Die Blockchain-Technologie und das Recht auf Vergessenwerden, NVwZ 2017, 1251 (1256)
[169] *Martini/Weinzierl*, Die Blockchain-Technologie und das Recht auf Vergessenwerden, NVwZ 2017, 1251 (1255).

(zentrale) Verantwortliche **keinen tatsächlichen Einfluss** auf die Datenverarbeitung der anderen Blockchain-Knoten, unabhängig ob diese schreibende oder nicht-schreibende Teilnehmer des Systems sind, bzw. auf deren Version der Datenkette hat. Deswegen ist (i) einerseits die Anzahl der nicht-schreibenden Teilnehmer, die „einfache" Betreiber von Blockchain-Knoten sind, zu beschränken (vgl. oben Punkt 4.d)ii)), und anderseits (ii) nicht nur die Kommunikation zwischen den Teilnehmern des Blockchain-Systems technisch oder organisatorisch zu gewährleisten ist, sondern auch (iii) die **rechtliche Einflussmacht** des (zentralen) Verantwortlichen auf die anderen Blockchain-Knoten als Teilnehmer des Blockchain-Systems, wie etwa Serviceanbieter, vorzusehen, welche die Erfüllung der Rechte der betroffenen Personen sichert.[170] Wird das Blockchain-System mehrere gemeinsam Verantwortlichen haben, ist auch eine rechtliche Verpflichtung der Verantwortlichen untereinander, die eine entsprechende Einflussmöglichkeit sichert, vorzusehen. Diese rechtliche Einflussmacht kann (i) durch den Abschluss einer (bzw. die Aufnahme in eine auch zu anderen Zwecken abzuschließende) **Vereinbarung** zwischen den Teilnehmern des Blockchain-Systems, etwa der Vereinbarung zwischen den gemeinsam Verantwortlichen oder der (jeweiligen) Auftragsverarbeitungsvereinbarung, sowie **alternativ** (ii) durch die Festlegung in einer **Verordnung** der Bundesministerin für Digitalisierung und Wirtschaftsstandort gesichert werden (vgl. zu den Rechtsinstrumenten bereits oben 4.c)ii) und 4.e)i)).

(2) Pflicht zur Information Dritter (Recht auf Vergessenwerden ieS)

Hat der zur Löschung verpflichtete Verantwortliche die personenbezogenen Daten ***„öffentlich gemacht"***, ist er verpflichtet, angemessene Maßnahmen zu treffen, um Dritte, die als Verantwortliche diese personenbezogenen Daten verarbeiten, *„darüber **zu informieren**, dass eine betroffene Person **von ihnen** die Löschung aller Links zu diesen personenbezogenen Daten oder von Kopien oder Replikationen dieser personenbezogenen Daten verlangt hat"*.[171] Es geht daher um die Informierung über ein gegenüber Dritten bestehendes Löschverlangen der betroffenen Person, das sich zumindest konkludent aus dem Löschantrag ergeben muss.[172]

Die personenbezogenen Daten sind *„öffentlich gemacht"*, wenn sie aktiv für die Öffentlichkeit, d.h. für die Allgemeinheit bzw. einen unbestimmten Personenkreis, zugänglich gemacht worden sind, was bei der Abrufbarkeit der Daten auf einer Webseite anzunehmen ist.[173] Eben dies, nämlich die Abrufbarkeit der Daten über eine Web-Oberfläche, wird bei der im Rahmen des Pilotprojekts entwickelten zentralen Datenbank für Personenzertifikate erfolgen, daher werden die Zertifikatsdaten öffentlich gemacht. Zu informieren sind folglich nicht nur die Teilnehmer des Blockchain-Systems, sondern **ein unüberschaubarer Kreis von Nutzern der zentralen**

---

[170] *Martini/Weinzierl*, Die Blockchain-Technologie und das Recht auf Vergessenwerden, NVwZ 2017, 1251 (1255 und 1257).
[171] Art 17 Abs 2 DSGVO.
[172] *Nolte/Werkmeister* in Gola, DS-GVO[2] Art 17 Rz 38f.
[173] *Nolte/Werkmeister* in Gola, DS-GVO[2] Art 17 Rz 36; *Haidinger* in Knyrim, DatKomm Art 17 DSGVO (Stand 1.10.2018, rdb.at) Rz 77.

Datenbank für Personenzertifikate als weitere Verantwortliche für die Verarbeitung der öffentlich gemachten personenbezogenen Daten.[174]

Diese Informationspflicht gilt allerdings nicht uneingeschränkt. Der zur Löschung verpflichtete Verantwortliche muss *„**unter Berücksichtigung der verfügbaren Technologien und der ihm zur Verfügung stehenden Mittel, angemessene Maßnahmen** – auch technischer Art – treffen, um die Verantwortlichen, die diese personenbezogenen Daten verarbeiten, über den Antrag der betroffenen Person zu informieren“*.[175] Zu setzen sind daher nur die Maßnahmen, die dem Verantwortlichen unter Berücksichtigung des Aufwands (Kosten, Personal, Zeit und Technik) zumutbar sind.[176] Als **unzumutbar** ist allerdings die Feststellung der Identität der Nutzer durch den Webseitenbetreiber (und deren anschließende Benachrichtigung) anzusehen, daher besteht keine Pflicht die Nutzer der zentralen Datenbank für Personenzertifikate zu identifizieren und über das Löschverlangen zu informieren.[177]

(3) Mitteilungspflicht

Vom oben dargestellten Pflicht zur Information Dritter ist die Mitteilungspflicht im Zusammenhang mit der Berichtigung oder Löschung personenbezogener Daten oder der Einschränkung der Verarbeitung zu unterscheiden. Diese **betrifft nicht die Datenübermittlung an einen unüberschaubaren Kreis von weiteren Verantwortlichen, sondern die gezielte Übermittlung an einen eingeschränkten Kreis von Datenempfängern**.[178]

Wie bereits oben ausgeführt, ist der Verantwortliche verpflichtet allen Empfängern, denen personenbezogene Daten offengelegt wurden, jede Berichtigung oder Löschung der personenbezogenen Daten sowie eine Einschränkung der Verarbeitung („korrigierende Veränderung“) mitzuteilen, *„es sei denn, dies erweist sich als unmöglich oder ist mit einem unverhältnismäßigen Aufwand verbunden“*.[179] Diese Nachberichtspflicht besteht somit nicht, wenn deren Erfüllung sich als (i) unmöglich, etwa wenn der Empfänger nicht mehr existent oder unbekannt ist, was bei Veröffentlichungen der Fall sein kann, oder (ii) als mit unverhältnismäßigem Aufwand verbunden erweist.[180] Im Rahmen der im Pilotprojekt entwickelten zentralen Datenbank für Personenzertifikate werden personenbezogene Daten zum Abruf bereitgestellt. Um sämtliche Empfänger dieser Daten von der Korrektur zu benachrichtigen, müsste ein automatisiertes Nachmeldeverfahren entwickelt werden, was selbst bei grundsätzlicher technischer

---

[174] *Nolte/Werkmeister* in Gola, DS-GVO[2] Art 17 Rz 37.
[175] ErwGr 67 Satz 2 DSGVO.
[176] *Nolte/Werkmeister* in Gola, DS-GVO[2] Art 17 Rz 40.
[177] *Nolte/Werkmeister* in Gola, DS-GVO[2] Art 17 Rz 40; ähnlich *Haidinger* in Knyrim, DatKomm Art 17 DSGVO (Stand 1.10.2018, rdb.at) Rz 81, wonach *„es einem Webseitenbetreiber nicht zumutbar [ist], alle anderen Webseitenbetreiber, die auf dessen Website verlinken, von der Löschung einer Information zielgerichtet zu verständigen“*.
[178] *Nolte/Werkmeister* in Gola, DS-GVO[2] Art 17 Rz 37.
[179] Art 19 Satz 1 DSGVO.
[180] *Gola* in Gola, DS-GVO[2] Art 19 Rz 7, 10; *Haidinger* in Knyrim, DatKomm Art 19 DSGVO (Stand 1.10.2018, rdb.at) Rz 16.

Umsetzbarkeit allerdings mit unverhältnismäßigen Aufwand verbunden wäre, daher entfällt die Nachberichtspflicht und die Berichtigung durch die Korrektur im Datenbestand des Verantwortlichen ist ausreichend.[181] Da bei der zentralen Datenbank für Personenzertifikate die aktive Nachberichtigung der Empfänger wegen Unverhältnismäßigkeit entfällt, ist der Verantwortliche auch nicht verpflichtet die betroffene Person über *„diese"* Empfänger zu unterrichten („Folgeunterrichtung"; vlg. zur Mittelungspflicht oben Punkt 4.f)ii)(2))).[182]

(4) Ausnahmen von Löschrechten und Informationspflicht

Zur Berücksichtigung der Interessen, welche der Löschung und der Information Dritter entgegenstehen, und das Recht der betroffenen Personen im Einzelfall einschränken können, werden in der DSGVO Ausnahmen vorgesehen.[183] Die weitere Speicherung der personenbezogenen Daten bleibt rechtmäßig, wenn dies (lit a) für die Ausübung des Rechts auf freie Meinungsäußerung und Information, (lit b) **zur Erfüllung einer rechtlichen Verpflichtung, die die Verarbeitung** nach dem Recht der Union oder der Mitgliedstaaten, dem der Verantwortliche unterliegt, **erfordert**, *„oder"* zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde („**Öffnungsklausel**"), (lit c) aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit, (lit d) für im öffentlichen Interesse liegende Archivzwecke, zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken oder (lit e) zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist.[184]

Eine Ausnahmeregelung von der Löschpflicht könnte man daher schaffen, indem man – im nationalen Recht – **eine rechtliche Verpflichtung zur Führung der zentralen Datenbank für Personenzertifikate** vorsieht. Diese Verpflichtung könnte sich nicht nur auf aktuelle und gültige Personenzertifikate, sondern auch auf die nicht mehr gültigen Zertifikate beziehen. Dies würde zur Speicherung von **historischen Zertifikatsdaten** berechtigen und das Recht der betroffenen Personen auf Löschung von Zertifikatsdaten nach Ablauf deren Gültigkeitsdauer ausschließen. Eine entsprechende Verpflichtung könnte mit einer (Register-)**Verordnung** der Bundesministerin für Digitalisierung und Wirtschaftsstandort eingeführt werden (vgl. oben Punkt 4.e)i)).

Alternativ wäre möglich, nach dem Vorbild des deutschen Bundesdatenschutzgesetzes („dBDSG")[185] im DSG den Einwand des unverhältnismäßigen Aufwands einzuführen.[186] Dieser

---

[181] Dies ist in der Literatur strittig, vlg. *Herbst* in Kühling/Buchner, DS-GVO/BDSG[2] Art 19 Rz 12, wonach sich das nicht pauschal beantworten lässt, sonder es vielmehr auf die Häufigkeit des Abrufens ankommt (mit weiteren Nachweisen der deutschen Literatur dafür und dagegen); für Unverhältnismäßigkeit iSd Art 19 DSGVO im Zusammenhang mit Blockchain auch *Finck*, Blockchains and Data Protection in the European Union, 22.

[182] Art 19 Satz 2 DSGVO; *Gola* in Gola, DS-GVO[2] Art 19 Rz 15; *Kamann/Braun* in Ehmann/Selmayr, DS-GVO Art 19 Rz 28.

[183] Art 17 Abs 3 DSGVO.

[184] ErwGr 65 Satz 5 DSGVO.

[185] Artikel 1 des Gesetzes vom 30.06.2017 (BGBl. I S. 2097), ins Kraft getreten am 25.05.2018.

[186] Vgl. § 35 dBDSG, allerdings nur für nicht automatisierte Verarbeitung.

könnte etwa als Satz 2 des § 4 Abs 2 DSG (vgl. dazu bereits oben Punkt 4.f)iv)(1)(c)) eingefügt werden, der anschließend etwa wie folgt lauten würde:

> **§ 4 Abs 2 DSG-NF:**
>
> *„Kann die Berichtigung oder Löschung von automationsunterstützt verarbeiteten personenbezogenen Daten nicht unverzüglich erfolgen, weil diese aus wirtschaftlichen oder technischen Gründen nur zu bestimmten Zeitpunkten vorgenommen werden kann, so ist die Verarbeitung der betreffenden personenbezogenen Daten mit der Wirkung nach Art. 18 Abs. 2 DSGVO bis zu diesem Zeitpunkt einzuschränken. Ebenso ist die Verarbeitung der betreffenden personenbezogenen Daten mit der Wirkung nach Art. 18 Abs. 2 DSGVO einzuschränken, wenn die Berichtigung oder Löschung wegen der besonderen Art der Verarbeitung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich und das Interesse der betroffenen Person an der Berichtigung oder Löschung als gering anzusehen ist."*

Die Voraussetzungen des Einwands des unverhältnismäßigen Aufwands wären bei der zentralen Datenbank für Personenzertifikate wegen der Speicherung der Daten in der Blockchain erfüllt. Die Aufnahme der Zertifikatsdaten in die zentrale Datenbank für Personenzertifikate würde auch nicht die Interessen der zertifizierten Personen als betroffenen Personen verletzen, sondern würde wegen leichterer Einsicht in die enthaltenen Zertifikate durch interessierte Unternehmen und Personen (wohl) deren Interessen an der leichten Auffindbarkeit und Überprüfbarkeit der Personenzertifikate fördern, daher wären ihre Interessen an der Löschung gering (vgl. oben Punkt 4.e)i)). Die Datenverarbeitung wäre aber in diesen Fällen einzuschränken, was auch zur Ende der Beauskunftung von betroffenen Zertifikaten führen würde.[187]

(5) Dispositionsfähigkeit des Rechts auf Löschung

Das Recht auf Löschung ist als subjektives Recht eine spezielle Ausprägung der Grundrechte auf Achtung des Privatlebens[188] und auf Schutz personenbezogener Daten[189]. Dieses Recht ist mit anderen Grundrechten wie etwa die unternehmerische Freiheit[190] und die Meinungs- und Informationsfreiheit[191] in Einklang zu bringen und daher nicht als absolutes, sondern als **relatives Recht** zu verstehen (vgl. auch oben Punkt 4.f)iv)(4)).[192]

---

[187] Für ein Recht auf Sperrung von personenbezogenen Daten als ein gelinderes Mittel auch *Schrey/Thalhofer*, Rechtliche Aspekte der Blockchain, NJW 2017, 1431 (1435).

[188] Art 7 Charta der Grundrechte der Europäischen Union, ABl. C 326 vom 26.10.2012, S. 391 („**GRC**").

[189] Art 8 GRC und Art 16 Vertrag über die Arbeitsweise der Europäischen Union, BGBl. III Nr. 86/1999 idgF. („**AEUV**"); Eine Prüfung des Informationseingriffes am Maßstab von 8 GRC führt zu keinem anderen Ergebnis als nach § 1 Abs 2 DSG, VfSlg 19.673/2012.

[190] Art 16 GRC.

[191] Art 11 GRC.

[192] *Nolte/Werkmeister* in Gola, DS-GVO[2] Art 17 Rz 4; *Kamann/Braun* in Ehmann/Selmayr, DS-GVO Art 17 Rz 9; *Finck*, Blockchains and Data Protection in the European Union, 24; ErwGr 1 DSGVO.

Von der grundsätzlichen Relativität ausgehend, stellt sich die Frage, ob betroffene Personen über das Rechts auf Löschung (und andere Rechte der betroffenen Personen) disponieren können. Für Österreich diese Frage – soweit ersichtlich – *bis dato* nicht näher untersucht und es existiert auch keine Judikatur hierzu.[193]

In deutscher Literatur wird zum Teil vertreten, dass das Recht auf Löschung aufgrund seines grundrechtlichen Charakters nicht privatrechtlich abbedungen oder eingeschränkt werden könne und sich dieses Recht ebenfalls der Disposition der betroffenen Person entziehe, was einen (einseitigen) Verzicht auf bzw. eine Einwilligung in die Beschränkung des Löschungsrechts *„unmöglich"* mache.[194] Diese Literaturmeinung basiert jedoch auf § 6 Abs 1 dBDSG a.F.[195], welche wie folgt lautete:

> *„Die Rechte des Betroffenen auf Auskunft (§§ 19, 34) und auf Berichtigung, Löschung oder Sperrung (§§ 20, 35) können nicht durch Rechtsgeschäft ausgeschlossen oder beschränkt werden."*

Diese Regelung wurde in die DSGVO nicht übernommen,[196] daher ist Frage nach der **Dispositionsfähigkeit des Rechts auf Löschung** (sowie auch der anderen Rechte der betroffenen Personen) entsprechend dem Schutzziel der Bestimmungen über Rechte der betroffenen Personen bzw. der DSGVO als Ganzes zu beantworten.

Die DSGVO schützt die Grundrechte und Grundfreiheiten natürlicher Personen bei der Verarbeitung ihrer personenbezogenen Daten, insbesondere ihr Recht auf Schutz personenbezogener Daten, ungeachtet ihrer Staatsangehörigkeit oder ihres Aufenthaltsorts (sowie den freien Verkehr personenbezogener Daten in der Union).[197]

Innerhalb der DSGVO bzw. des Systems des Datenschutzrechts zählen die Rechte der betroffenen Personen, so auch das Recht auf Löschung, zu den klassischen Instrumenten des Selbst-Datenschutzes.[198] Durch die DSGVO wollte der Verordnungsgeber die Rechtsstellung der betroffenen Personen im Datenschutzrecht betonen und weiter stärken, wozu auch die Anerkennung der Herrschaft des Einzelnen über seine (personenbezogenen) Daten zählt, die einerseits die Möglichkeit zur effektiven Rechtsdurchsetzung voraussetzt und anderseits die Verantwortung für die eigenen Daten der betroffenen Person aufträgt und auch zumutet.[199] Die Abwägung des Rechts auf Datenschutz – sowie des Rechts auf Achtung des Privatlebens – mit andern (nach der DSGVO ebenfalls zu berücksichtigenden) Rechten, wie etwa die unternehmerische Freiheit, Meinungs- und Informationsfreiheit sowie Recht auf informationelle Selbstbestimmung steht daher in erster Linie der betroffenen Person zu.[200]

---

[193] *Haidinger/Illibauer* in Knyrim, DatKomm Vor Kapitel III DSGVO (Stand 1.10.2018, rdb.at) Rz 3.
[194] *Schrey/Thalhofer*, Rechtliche Aspekte der Blockchain, NJW 2017, 1431 (1435); *Kamann/Braun* in Ehmann/Selmayr, DS-GVO Art 17 Rz 8.
[195] Bundesdatenschutzgesetz in der bis zum 24. Mai 2018 geltenden Fassung.
[196] *Schrey/Thalhofer*, Rechtliche Aspekte der Blockchain, NJW 2017, 1431 (1435).
[197] Art 1 DSGVO, ErwGr 2 DSGVO.
[198] *Worms* in Wolff/Brink, BeckOK Datenschutzrecht (26. Edition, Stand: 01.08.2018) Art 16 Rz 2.
[199] *Worms* in Wolff/Brink, BeckOK Datenschutzrecht (26. Edition, Stand: 01.08.2018) Art 16 Rz 3ff.
[200] Vgl. ErwGr 4 DSGVO.

Aus diesen Gründen ist bei der Beurteilung der Dispositionsfähigkeit des Rechts auf Löschung (zumindest) eine **differenzierende Betrachtung** angebracht. Die betroffene Person kann unseres Erachtens in Verfolgung ihrer anderen Grundrechte und Grundfreiheiten und/oder sonstigen legitimen Interessen (wohl) im Einzelfall über ihr Recht auf Löschung (sowie andere datenschutzbezogene Rechte) disponieren, soweit dies ein geeignetes und erforderliches Mittel zur Erreichung eines dieser Interessen ist und nach Abwägung des Nutzens für die betroffene Person und der Beeinträchtigung ihrer grundrechtlich geschützten Position angemessen ist. Letzteres ist – im Sinne der Herrschaft des Einzelnen über seine (personenbezogenen) Daten und des Rechts auf informationelle Selbstbestimmung – aus der Perspektive der betroffenen Person zu beurteilen, wobei ihre subjektiven Vorstellungen und Wertungen in die Abwägung einzufließen haben.

Die im Rahmen des Pilotprojekts entwickelte **zentrale Datenbank für Personenzertifikate** wird der möglichst effizienten Erteilung von Auskünften über Personenzertifikate an die Öffentlichkeit dienen, weil ihre Entwicklung die Beauskunftung wesentlich vereinfachen und beschleunigen wird. Der Aufbau der zentralen Datenbank für Personenzertifikate fördert daher wegen der Vereinfachung der Einsicht in die in der Datenbank enthaltenen Zertifikate durch interessierte Unternehmen und Personen die Interessen der zertifizierten Personen an der leichten Auffindbarkeit und Überprüfbarkeit der Personenzertifikate (vgl. oben Punkt 4.e)i)). Ist im Blockchain-System, auf welchem die im Rahmen des Pilotprojekts entwickelte Datenbank basieren wird, die Löschung der personenbezogenen Daten (technisch) nicht – oder nur mit unverhältnismäßigen Aufwand – umsetzbar (vgl dazu oben Punkt 4.f)iv)(1)(c)), ist **die Einwilligung in die Beschränkung des Rechts auf Löschung bzw. der Verzicht der zertifizierten Personen auf Löschung** von deren personenbezogenen (Zertifikats-)Daten, etwa nach Ablauf der Gültigkeit eines Zertifikats oder nach Berichtigungen der Zertifikatsdaten durch Eintragung eines neuen Blocks in die Blockchain, ein geeignetes und erforderliches Mittel, um die Verarbeitung von personenbezogenen Zertifikatsdaten in der Blockchain zu ermöglichen und dadurch die legitimen Interessen der zertifizierten Person zu verwirklichen.

Die Einwilligung in die Beschränkung des Rechts auf Löschung (oder eines anderen Rechts der betroffenen Person) bzw. die diesbezügliche Verzichtserklärung der betroffenen Person hat unseres Erachtens **die gleichen (datenschutzrechtlichen) Anforderungen wie eine Einwilligung** in die Verarbeitung der sie betreffenden personenbezogenen Daten **gemäß Art 4 Nr 11 DSGVO** zu erfüllen und daher vor allem freiwillig für den bestimmten Fall und in informierter Weise zu erfolgen. Ähnlich wie bei einer Einwilligung ist der Widerruf des Verzichts jedoch nach dem Prinzip von Treu und Glauben ausgeschlossen, wenn die Erfüllung des Rechts, auf welches verzichtet wurde, (technisch) nicht mehr möglich ist.[201] Die betroffene Person ist vor der Abgabe der Verzichtserklärung über diesen Umstand in Kenntnis zu setzen.

[201] *Schulz* in Gola, DS-GVO[2] Art 7 Rz 57.

Um den Interessen der betroffenen Person im größtmöglichen Umfang Rechnung zu tragen, ist **die Verarbeitung** von Daten, welche mangels Verzichts zu löschen wären, jedoch beim Vorliegen eines Löschgrundes **einzuschränken** (vgl. dazu oben zur Löschgründen 4.f)iv)(1)(a) und zur Einschränkung der Verarbeitung 4.f)iv)(1)(c)).

v) Beschränkung der Rechte der betroffenen Personen

Die zentrale Regelung für den Erlass von nationalen Rechtsvorschriften, die bestimmte Rechte der betroffenen Personen beschränken, ist Art 23 DSGVO.[202] Dieser sieht einen umfangreichen Katalog an Öffnungsklauseln vor, die dem **nationalen Gesetzgeber die Befugnis** geben, aus gewissen taxativ aufgezählten Gründen die Rechte der betroffenen Personen und zwar auf Unterrichtung, Auskunft zu und Berichtigung oder Löschung personenbezogener Daten, auf Datenübertragbarkeit und auf Widerspruch, Entscheidungen, die auf der Erstellung von Profilen beruhen, sowie Mitteilungen über eine Verletzung des Schutzes personenbezogener Daten an eine betroffene Person, und bestimmte damit zusammenhängende Pflichten der Verantwortlichen **einzuschränken** sowie die damit (allenfalls) einhergehende Einschränkung von Grundsätzen der Datenverarbeitung vorzunehmen.[203]

Die Einschränkungen der Rechte der betroffenen Personen können nur zur Verfolgung folgender Ziele vorgenommen werden: (lit a) die nationale Sicherheit, (lit b) die Landesverteidigung, (lit c) die öffentliche Sicherheit, (lit d) die Maßnahmen des Strafrechts und -vollstreckungsrechts einschließlich Gefahrenabwehr, (lit e) **die sonstigen wichtigen Ziele des allgemeinen öffentlichen Interesses der Union oder eines Mitgliedstaats**, etwa wichtige wirtschaftliche oder finanzielle Interessen („Generalklausel"), (lit f) der Schutz der Unabhängigkeit der Justiz und den Schutz von Gerichtsverfahren, (lit g) der Schutz der berufsständischen Regeln reglementierter Berufe, (lit h) die Kontroll-, Überwachungs- und Ordnungsfunktionen, (lit i) der Schutz der betroffenen Person oder der Rechte und Freiheiten anderer Personen, etwa einer nicht geschäftsfähigen betroffenen Person, oder (lit j) die Durchsetzung zivilrechtlicher Ansprüche.[204]

Ein (legitimer) Ziel iSd lit e ist ***„das Führen öffentlicher Register aus Gründen des allgemeinen öffentlichen Interesses"***.[205] Da die zentrale Datenbank für Personenzertifikate der Erteilung von Auskünften an die Öffentlichkeit und somit dem allgemeinen öffentlichen Interesse dienen wird, kann davon ausgegangen werden, dass eine derartige öffentlich zugängliche Datenbank ein öffentliches Register iSd Art 23 Abs 1 lit e DSGVO darstellt und **die Einschränkung der Rechte der betroffenen Personen durch nationale Rechtsvorschriften grundsätzlich zulässig ist**.

---

[202] *Bertermann* in Ehmann/Selmayr, DS-GVO[2] Art 23 Rz 1.
[203] Art 23 Abs 1 DSGVO, ErwGr 73 Satz 1 DSGVO.
[204] Art 23 Abs 1 DSGVO, ErwGr 73 Satz 1 DSGVO; *Bäcker* in Kühling/Buchner, DS-GVO/BDSG[2] Art 23 Rz 9.
[205] ErwGr 73 Satz 1 DSGVO; *Gola* in Gola, DS-GVO[2] Art 23 Rz 9.

Bei der nationalen Rechtsvorschrift muss es sich nicht unbedingt um einen vom Parlament angenommenen Rechtsakt, also ein **Gesetz** im formellen Sinn, handeln.[206] Notwendig ist allerdings, dass der Rechtsakt Außenwirksamkeit durch eine amtliche Veröffentlichung erlangt.[207] Die Einschränkung kann daher grundsätzlich auch durch Verordnungen von Verwaltungsbehörden gemäß Art 18 Abs 2 B-VG, etwa eine (Register-)**Verordnung** der Bundesministerin für Digitalisierung und Wirtschaftsstandort, erfolgen.[208]

Die durch nationale Rechtsvorschrift vorgesehene Einschränkung muss den **Wesensgehalt der Grundrechte** und Grundfreiheiten achten sowie in einer demokratischen Gesellschaft eine **notwendige und verhältnismäßige** Maßnahme darstellen, daher wäre eine „pauschale" Ausnahme von der Pflicht, sämtliche oder einzelne Rechte der betroffenen Personen zu erfüllen, unzulässig.[209] Die Einschränkung sollte einerseits mit der Charta der Grundrechte der Europäischen Union und mit der Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten im Einklang stehen.[210] Anderseits sind bei Einschränkung des Rechts auf Auskunft, des Rechts auf Richtigstellung und des Rechts auf Löschung, das (nationale) Grundrecht auf Datenschutz bzw. Voraussetzungen für einen Eingriff in dieses Grundrecht zu berücksichtigen (vgl. § 1 Abs 4 iVm Abs 2 DSG). Die Eingriffsvoraussetzungen entsprechen dem Art 8 Abs 2 EMRK und sind mit denen des Art 23 DSGVO vergleichbar.[211]

Die nationale Rechtsvorschrift, mit welcher die Einschränkung von Rechten der betroffenen Personen vorgesehen wird, muss sich insbesondere beziehen auf (lit a) die Zwecke der Verarbeitung oder die Verarbeitungskategorien, (lit b) die Kategorien personenbezogener Daten, (lit c) den Umfang der vorgenommenen Beschränkungen, (lit d) die Garantien gegen Missbrauch oder unrechtmäßigen Zugang oder unrechtmäßige Übermittlung, (lit e) die Angaben zu dem Verantwortlichen oder den Kategorien von Verantwortlichen, (lit f) die jeweiligen Speicherfristen sowie die geltenden Garantien unter Berücksichtigung von Art, Umfang und Zwecken der Verarbeitung oder der Verarbeitungskategorien, (lit g) die Risiken für die Rechte und Freiheiten der betroffenen Personen und (lit h) das Recht der betroffenen Personen auf Unterrichtung über die Beschränkung, sofern dies nicht dem Zweck der Beschränkung abträglich ist.[212] Es handelt sich dabei um **Mindestanforderungen**, welche grundsätzlich **kumulativ** bestehen.[213]

Ob die oben geschilderten Voraussetzungen erfüllt sind, muss im Einzelfall anhand vom konkret einzuschränkenden Recht der betroffenen Personen und der Ausgestaltung der Beschränkung beurteilt werden. Der Wesensgehalt des Rechts auf Löschung bleibt unseres Erachtens (jedenfalls) gewährt, wenn die Verarbeitung von Daten, welche mangels Beschränkung beim

---

[206] ErwGr 41 Satz 1 DSGVO.
[207] *Bertermann* in Ehmann/Selmayr, DS-GVO[2] Art 23 Rz 6 mwN.
[208] *Haidinger* in Knyrim, DatKomm Art 23 DSGVO (Stand 1.10.2018, rdb.at) Rz 8.
[209] Art 23 Abs 1 DSGVO; *Bertermann* in Ehmann/Selmayr, DS-GVO[2] Art 23 Rz 3f.
[210] ErwGr 73 Satz 2 DSGVO.
[211] *Haidinger* in Knyrim, DatKomm Art 23 DSGVO (Stand 1.10.2018, rdb.at) Rz 6, 9; zur deutschen Rechtslage etwa *Bertermann* in Ehmann/Selmayr, DS-GVO[2] Art 23 Rz 4.
[212] Art 23 Abs 2 DSGVO.
[213] *Gola* in Gola, DS-GVO[2] Art 23 Rz 3.

Vorliegen eines Löschgrundes zu löschen wären, in diesen Fällen eingeschränkt wird, und die vorgesehenen Garantien daher (zumindest aus der Perspektive der interessierten Öffentlichkeit) der wirkungsorientierten Löschung iSd DSGVO nahekommen (vgl. oben Punkt 4.f)iv)(1)(b)). Ist im Blockchain-System, auf welchem die im Rahmen des Pilotprojekts entwickelte zentrale Datenbank für Personenzertifikate basieren wird, die Löschung der personenbezogenen Daten (technisch) nicht – oder nur mit unverhältnismäßigen Aufwand – umsetzbar (vgl dazu oben Punkt 4.f)iv)(1)(c)), ist die Beschränkung des Rechts auf Löschung eine notwendige und verhältnismäßige Maßnahme, um die Verarbeitung von personenbezogenen Zertifikatsdaten in der Blockchain zu ermöglichen und dadurch die legitimen Interessen der zertifizierten Person an der leichten Auffindbarkeit und Überprüfbarkeit der Personenzertifikate zu verwirklichen (vgl. oben Punkt 4.e)i)). Eine Einwilligung der zertifizierten Personen als betroffenen Personen in die Beschränkung des Rechts auf Löschung bzw. ein Verzicht auf ihr Recht ist im Fall einer Beschränkung durch eine Rechtsvorschrift nicht erforderlich.

Die oben dargestellten Mindestanforderungen überlappen sich teilweise mit dem möglichen Inhalt einer Verordnung (oder sonstiger Rechtsvorschrift), die (unter anderen) eine rechtliche Verpflichtung der Zertifizierungsstellen für Personen und der Akkreditierung Austria zur Führung einer zentralen Datenbank für Personenzertifikate vorsehen und als Legitimationsgrundlage bzw. Rechtgrundlage der Datenverarbeitung in der zentralen Datenbank für Personenzertifikate dienen könnte (vgl. oben Punkt 4.e)i)).[214] Sollte eine nationale Rechtsvorschrift nicht nur die Zulässigkeit der Verarbeitung, sondern ferner die Rechte der betroffenen Personen bzw. die Pflichten der Verantwortlichen einschränken, sind die oben geschilderte Voraussetzungen der Öffnungsklausel gemäß Art 23 DSGVO einzuhalten (vgl. oben Punkt 4.e)i)).[215]

Ferner ist zu beachten, dass die DSGVO eine **weitere Öffnungsklausel** vorsieht, aufgrund welcher Ausnahmen vom Recht auf Löschung vorgesehen werden können, wenn dies zur Erfüllung einer rechtlichen Verpflichtung, die die Verarbeitung nach dem Recht der Union oder der Mitgliedstaaten, dem der Verantwortliche unterliegt, verlangt, erforderlich ist (vgl. oben Punkt 4.f)iv)(4)).[216] Diese Öffnungsklausel ist *lex spezialis* gegenüber der breiteren Öffnungsklausel gemäß Art 23 DSGVO.[217] Damit ist allerdings nicht ausgeschlossen, dass über den Anwendungsbereich der spezifischeren Öffnungsklausel hinaus weitere Beschränkungen des Rechts auf Löschung vorgesehen werden, die dann aber den strengeren Anforderungen des Art 23 DSGVO genügen müssen.[218]

[214] ErwGr 45 Satz 5 DSGVO.
[215] *Schulz* in Gola, DS-GVO[2] Art 6 Rz 42.
[216] Art 17 Abs 3 lit b DSGVO.
[217] *Haidinger* in Knyrim, DatKomm Art 23 DSGVO (Stand 1.10.2018, rdb.at) Rz 2; *Feiler/Forgó*, EU-DSGVO Art 23 Rz 1.
[218] *Haidinger* in Knyrim, DatKomm Art 23 DSGVO (Stand 1.10.2018, rdb.at) Rz 2.