EUROPÄISCHE
KOMMISSION

Brüssel, den 24.7.2019
COM(2019) 372 final

BERICHT DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT UND DEN RAT

über die Vernetzung der zentralen automatischen Mechanismen (zentrale Register oder zentrale elektronische Datenabrufsysteme) der Mitgliedstaaten für Bankkonten

BERICHT DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT UND DEN RAT

über die Vernetzung der zentralen automatischen Mechanismen (zentrale Register oder zentrale elektronische Datenabrufsysteme) der Mitgliedstaaten für Bankkonten

1. Einleitung

Gemäß Artikel 32a der Geldwäscherichtlinie (EU) 2015/849/EU[1] müssen die Mitgliedstaaten bis zum 10. September 2020 zentrale automatische Mechanismen wie zentrale Register oder zentrale elektronische Datenabrufsysteme einrichten, die die Ermittlung aller natürlichen oder juristischen Personen ermöglichen, die Zahlungskonten, Bankkonten und Schließfächer innehaben oder kontrollieren. Die Geldwäscherichtlinie legt eine Mindestauswahl an Informationen fest, die in diese zentralen Mechanismen aufzunehmen sind. Ferner sieht die Richtlinie vor, dass die zentralen Meldestellen sofort und ungefiltert auf diese Mechanismen zugreifen können, wobei auch die anderen zuständigen Behörden Zugang zu den Informationen erhalten müssen, damit sie ihren Pflichten im Rahmen der Geldwäscherichtlinie nachkommen können. Die Richtlinie (EU) 2019/1153 zur Erleichterung des Zugangs zu Finanz- und sonstigen Informationen[2] verpflichtet die Mitgliedstaaten, die für die Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten zuständigen nationalen Behörden zu benennen, die unmittelbar, sofort und ungefiltert Zugang zu der Mindestauswahl an Informationen aus solchen zentralen Mechanismen erhalten. Zu diesen zuständigen Behörden zählen mindestens die Vermögensabschöpfungsstellen.

Der Zugang der zuständigen Behörden zu zentralen Bankkontenregistern oder Abrufsystemen wird eine wichtige Rolle beim Kampf gegen Geldwäsche, damit zusammenhängende Vortaten und Terrorismusfinanzierung sowie allgemein bei der Bekämpfung schwerer Straftaten spielen. Angesichts der Ziele der Geldwäscherichtlinie und der Richtlinie zur Erleichterung des Zugangs zu Finanz- und sonstigen Informationen würde eine künftige EU-weite Vernetzung von Bankkontenregistern und Datenabrufsystemen die grenzübergreifende Zusammenarbeit der am Kampf gegen Geldwäsche, Terrorismusfinanzierung und anderen schweren Straftaten beteiligten zuständigen Behörden erleichtern.

Gemäß Artikel 32a Absatz 5 der Geldwäscherichtlinie hat die Kommission die Bedingungen und technischen Spezifikationen und Verfahren für die Gewährleistung einer sicheren und effizienten Vernetzung der zentralen automatischen Mechanismen zu bewerten. In diesem Bericht werden daher die verschiedenen IT-Lösungen auf EU-Ebene bewertet, die entweder bereits verwendet werden oder sich im Entwicklungsstadium befinden und die als Vorbilder für eine mögliche Vernetzung der

[1] Richtlinie (EU) 2015/849 des Europäischen Parlaments und des Rates vom 20. Mai 2015 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung, zur Änderung der Verordnung (EU) Nr. 648/2012 des Europäischen Parlaments und des Rates und zur Aufhebung der Richtlinie 2005/60/EG des Europäischen Parlaments und des Rates und der Richtlinie 2006/70/EG der Kommission (ABl. L 849 vom 9.7.2018, S. 1).

[2] Richtlinie (EU) 2019/1153 des Europäischen Parlaments und des Rates vom 20. Juni 2019 zur Festlegung von Vorschriften zur Erleichterung der Nutzung von Finanz- und sonstigen Informationen für die Verhütung, Aufdeckung, Untersuchung oder Verfolgung bestimmter Straftaten und zur Aufhebung des Beschlusses 2000/642/JI des Rates (ABl. L 186 vom 11.7.2019, S. 122).

zentralen Mechanismen dienen könnten. Für eine erfolgreiche Vernetzung wäre ein Rechtsinstrument erforderlich.

Dieser Bericht sollte in Verbindung mit dem supranationalen Risikobewertungsbericht der Kommission[3], dem Bericht der Kommission über die zentralen Meldestellen[4] und dem Bericht der Kommission über die Bewertung aktueller Fälle von mutmaßlicher Geldwäsche unter Beteiligung von Kreditinstituten aus der EU[5] betrachtet werden, die gleichzeitig vorgelegt werden.

2. Aktueller Stand

2.1. Zentrale Register oder elektronische Datenabrufsysteme für Bankkonten in den Mitgliedstaaten

Bislang[6] gibt es in 15 Mitgliedstaaten[7] zentrale Mechanismen, die Informationen über Bankkonten enthalten. Die Antworten der Mitgliedstaaten lassen eine leichte Präferenz zugunsten der technischen Lösung des zentralen Registers erkennen: Während 17 Mitgliedstaaten zentrale Register haben oder in Kürze haben werden, gaben neun Mitgliedstaaten an, zentrale Datenabrufsysteme zu nutzen oder in Zukunft nutzen zu wollen[8]. Eine Präferenz gibt es auch zugunsten von Systemen, die zusätzlich zu den in Artikel 32a Absatz 5 der 5. Geldwäscherichtlinie vorgeschriebenen Mindestangaben zum Kontoprofil weitere Informationen enthalten (11 Anworten von 17)[9].

[3] Bericht der Kommission an das Europäische Parlament und den Rat über die Bewertung der mit grenzüberschreitenden Tätigkeiten im Zusammenhang stehenden Risiken der Geldwäsche und der Terrorismusfinanzierung für den Binnenmarkt (COM(2019) 370).
[4] Bericht der Kommission an das Europäische Parlament und den Rat über die Bewertung des Rahmens für die Zusammenarbeit zwischen den zentralen Meldestellen für Geldwäsche-Verdachtsanzeigen (FIU) (COM(2019) 371).
[5] Bericht der Kommission an das Europäische Parlament und den Rat über die Bewertung aktueller Fälle von mutmaßlicher Geldwäsche unter Beteiligung von Kreditinstituten aus der EU (COM(2019) 373).

[6] Die Informationen in diesem Abschnitt beruhen auf den Antworten der Mitgliedstaaten auf einen Fragebogen, der ihnen im März 2019 zugesandt wurde, auf Informationen aus dem von der Kommission veranstalteten Umsetzungs-Workshop vom 1. April 2019 und auf den Anhang 7 der Folgenabschätzung zu dem Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zur Festlegung von Vorschriften zur Erleichterung der Nutzung von Finanz- und sonstigen Informationen für die Verhütung, Aufdeckung, Untersuchung oder Verfolgung bestimmter Straftaten und zur Aufhebung des Beschlusses 2000/642/JI des Rates (SWD(2018) 114 final).
[7] Belgien, Bulgarien, Tschechien, Deutschland, Griechenland, Spanien, Frankreich, Kroatien, Italien, Lettland, Litauen, Österreich, Portugal, Rumänien, Slowenien. Die Slowakei verfügt über ein zentrales elektronisches Datenabrufsystem, das derzeit jedoch nur für Amtspersonen zugänglich ist.
[8] Finnland zählt zu beiden Gruppen, da es demnächst ein System einsetzen wird, das beide Lösungen verwendet. Bei einem zentralen Register werden die einschlägigen Informationen in einer einzigen zentralen Datenbank gesammelt und aufbewahrt, während ein zentrales elektronisches Datenabrufsystem aus einem zentralen IT-Portal besteht, das Informationen aus verschiedenen zugrunde liegenden Datenbanken (die beispielsweise von Finanzinstituten gepflegt werden) abruft.
[9] Laut den Antworten der Mitgliedstaaten können diese zusätzlichen Informationen Angaben über vom Kontoinhaber abgeschlossene Finanzkontrakte oder über Transaktionen, die im Zusammenhang mit dem Konto getätigt wurden, umfassen.

2.2. EU-Systeme zur Vernetzung nationaler dezentraler elektronischer Datenbanken

Es gibt mehrere EU-Projekte, die die EU-weite dezentrale Vernetzung nationaler elektronischer Datenbanken gewährleisten.[10] Folgende IT-Systeme gelten für diesen Bericht als relevant:

Das Europäische Strafregisterinformationssystem (ECRIS) wurde im April 2012 in Betrieb genommen, um den Austausch von Strafregisterinformationen in der gesamten EU zu verbessern.[11] Alle Mitgliedstaaten sind derzeit an ECRIS angeschlossen. ECRIS gewährleistet, dass Informationen über Verurteilungen zwischen den Mitgliedstaaten auf einheitliche, schnelle und kompatible Weise ausgetauscht werden, und bietet Richtern und Staatsanwälten leichten Zugang zu umfassenden Informationen über die Vorstrafen der betreffenden Personen.[12]

Über das Europäische Fahrzeug- und Führerschein-Informationssystem (EUCARIS) können die Länder Informationen über Fahrzeuge und Führerscheine sowie andere verkehrsbezogene Daten austauschen. EUCARIS ist ein Mechanismus, über den die Zulassungsbehörden für Kraftfahrzeuge und Führerscheine in der Union miteinander verbunden sind und Informationen zu Fahrzeugeigentümern und Fahrzeugversicherungen zwischen den nationalen Kontaktstellen der Mitgliedstaaten ausgetauscht werden können.[13]

Die EU-weite Vernetzung der Insolvenzregister (IRI) umfasst zwei verschiedene Projekte. Die erste Version des Systems (IRI 1.0) ist seit Juli 2014 über das Europäische Justizportal[14] zugänglich. Sie wurde als Pilotprojekt[15] entwickelt und basiert auf der freiwilligen Teilnahme bestimmter Mitgliedstaaten[16]. Die zweite Version (IRI 2.0) stützt sich auf die Verordnung (EU) 2015/848 über Insolvenzverfahren und wird die nationalen Insolvenzregister aller Mitgliedstaaten (mit Ausnahme Dänemarks) vernetzen. Bis Juni 2021 sollen alle Mitgliedstaaten daran teilnehmen. Während IRI 1.0 auf einem standardisierten sicheren Webdienst zum Austausch von Nachrichten (SOAP über HTTPS)

[10]Zentrale IT-Systeme mit einheitlichen Datenbanken auf EU-Ebene, wie das Schengener Informationssystem oder das Visa-Informationssystem, sind von der Bewertung ausgenommen, da solche Systeme mit auf nationaler Ebene bestehenden zentralen Datenbanken unvereinbar sind.

[11]Rahmenbeschluss 2009/315/JI des Rates vom 26. Februar 2009 über die Organisation und den Inhalt des Austauschs von Strafregisterinformationen zwischen den Mitgliedstaaten und Beschluss 2009/316/JI des Rates vom 6. April 2009 zur Einrichtung des Europäischen Strafregisterinformationssystems (ECRIS) gemäß Artikel 11 des Rahmenbeschlusses 2009/315/JI – geändert durch die Richtlinie (EU) 2019/884 des Europäischen Parlaments und des Rates vom 17. April 2019 im Hinblick auf den Austausch von Informationen über Drittstaatsangehörige und auf das Europäische Strafregisterinformationssystem (ECRIS).

[12]Im April 2019 wurde eine neue EU-Rahmenregelung verabschiedet, mit der ECRIS durch einen Mechanismus ergänzt werden soll, der einen effizienten Austausch von Strafregisterinformationen über Drittstaatsangehörige ermöglicht, die im Hoheitsgebiet der EU verurteilt wurden. Dieses Europäische Strafregisterinformationssystem für Drittstaatsangehörige (ECRIS-TCN), ein zentralisiertes System zur Ermittlung von Treffern beim Datenabgleich, wird ausschließlich die zur Identifizierung von verurteilten Drittstaatsangehörigen erforderlichen Daten und die Angabe des Mitgliedstaats, in dem diese zuvor verurteilt wurden, enthalten. Bei Treffern muss der ersuchende Mitgliedstaat dann die Informationen über die Verurteilung selbst bei dem vom ECRIS-TCN angegebenen Mitgliedstaat über das bestehende ECRIS anfordern.

[13] Rechtsgrundlagen für den Prüm-Dienst von EUCARIS sind der Beschluss 2008/615/JI des Rates vom 23. Juni 2008 zur Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus und der grenzüberschreitenden Kriminalität, und der Beschluss 2008/616/JI des Rates zur Durchführung des Beschlusses 2008/615/JI.

[14]https://beta.e-justice.europa.eu/246/EN/bankruptcy_amp_insolvency_registers__search_for_insolvent_firms_in_the_eu

[15]Das Pilotprojekt wurde auf der Grundlage des Mehrjährigen Aktionsplans für die europäische E-Justiz 2009-2013 (ABl. C 75 vom 31.3.2009, S. 1) und des Mehrjährigen Aktionsplans für die europäische E-Justiz 2014-2018 (ABl. C 182 vom 14.6.2014, S. 2) umgesetzt und ausgeführt.

[16]Derzeit nehmen Tschechien, Deutschland, Estland, Italien, Lettland, die Niederlande, Österreich, Rumänien und Slowenien teil.

basiert, fördert IRI 2.0 zusätzlich den Datenaustausch, indem es den eDelivery-Baustein der Fazilität „Connecting Europe“ (CEF)[17] unterstützt.

Das System zur Verknüpfung von Unternehmensregistern (BRIS) dient der Vernetzung von Unternehmensregistern zum grenzüberschreitenden Austausch von Nachrichten über Fusionen und Zweigstellen und ermöglicht den Nutzern des E-Justiz-Portals, auf mehrsprachige Informationen über EU-Unternehmen zuzugreifen. Das System erfüllt die Bestimmungen hinsichtlich der Vernetzung von Zentral-, Handels- und Gesellschaftsregistern gemäß der Richtlinie 2012/17/EU[18] und ist seit Juni 2017 in Betrieb. Für den Austausch standardisierter Mitteilungen nutzt BRIS den eDelivery-Baustein der Fazilität „Connecting Europe“. Das dezentrale System verfügt über eine zentrale Komponente (die zentrale Europäische Plattform), die Namen von Unternehmen und Registernummern speichert und indexiert.

Die Anwendung „Vernetzung der Grundbücher“ (LRI) ist ein laufendes Projekt[19] auf freiwilliger Basis, das innerhalb des Europäischen Justizportals den einzigen Zugangspunkt zu den Grundbüchern der teilnehmenden EU-Länder bilden soll. Die Inbetriebnahme ist für das zweite Quartal des Jahres 2020 geplant.

Die „European Business Ownership and Control Structures“ (europäische Strukturen für Unternehmensbesitz und -kontrolle – EBOCS) ist ein Projekt, das von der „European Business Registers Association“ (Verband europäischer Unternehmensregister) mit finanzieller Unterstützung aus dem Fonds für die innere Sicherheit (ISF) – Polizei durchgeführt wird (Jahresarbeitsprogramme 2016 und 2018). Über die EBOCS-Plattform wird ein vereinfachter und einheitlicher Zugang zu Daten aus Unternehmensregistern über Besitz- und Kontrollstrukturen von Unternehmen zur Erstellung von Finanzanalysen und für Untersuchungszwecke zur Verfügung gestellt. Zudem kann sich der Nutzer der Plattform die zusammengefassten Abfrageergebnisse in einer Grafik anzeigen lassen. Es sei darauf hingewiesen, dass die EU nicht über die Urheberrechte an diesem System verfügt.

Das e-CODEX-System (Kommunikation im Rahmen des elektronischen Rechtsverkehrs mit Hilfe von Online-Datenaustausch) erleichtert – über ein dezentrales System für den grenzüberschreitenden Austausch elektronischer Mitteilungen im Bereich der Justiz – die sichere Kommunikation in zivil- und strafrechtlichen Verfahren.[20] Derzeit erleichtert e-CODEX im Rahmen eines Pilotversuchs zum Europäischen Zahlungsbefehl und zum europäischen Verfahren für geringfügige Forderungen die elektronische Kommunikation zwischen Bürgern und Gerichten sowie zwischen den Verwaltungen der Mitgliedstaaten. Im Bereich Strafjustiz ist e-CODEX zudem die bevorzugte Lösung für das „e-

[17] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eDelivery

[18] Richtlinie 2012/2017/EU des Europäischen Parlaments und des Rates vom 13. Juni 2012 zur Änderung der Richtlinie 89/666/EWG des Rates sowie der Richtlinien 2005/56/EG und 2009/101/EG des Europäischen Parlaments und des Rates in Bezug auf die Verknüpfung von Zentral-, Handels- und Gesellschaftsregistern (ABl. L 156 vom 16.6.2012, S. 1).

[19] Für die Vernetzung besteht keine Rechtsgrundlage; LRI ist ein freiwilliges System, an dem sich die Mitgliedstaaten beteiligen können.

[20] Das e-CODEX-System besteht aus einem Softwarepaket (CEF eDelivery und e-CODEX connector), das zur Einrichtung eines Zugangspunkts auf nationaler Ebene eingesetzt werden kann, um eine sichere Kommunikation zu gewährleisten. Es handelt sich dabei nicht um ein System zur Verknüpfung nationaler Datenbanken oder Register, sondern um eine Kommunikationsinfrastruktur, die die sichere Kommunikation und den sicheren Informationsaustausch zwischen den nationalen IT-Systemen gewährleistet und als solche für die Bewertung in diesem Bericht relevant ist. e-CODEX wurde von 2010 bis 2016 von 21 Mitgliedstaaten unter Beteiligung anderer Länder/Gebiete und Organisationen entwickelt.

Evidence Digital Exchange System“[21], d. h. für den Online-Austausch von elektronischen Beweismitteln im Rahmen der Europäischen Ermittlungsanordnung (EEA) und der Rechtshilfeabkommen.

3. Hauptparameter

3.1. Zugangsvoraussetzung für Nutzer

Ein Blick auf die bestehenden Systeme zeigt, dass sich der Zugang zu dem System, das mit dem vernetzten IT-System interagiert, auf der Nutzerseite nach dem Zweck bestimmt, für den es eingerichtet wurde. Soll mit der Vernetzung die Transparenz der Informationen für Unternehmen im Binnenmarkt (BRIS, IRI) verbessert werden, ist das System öffentlich zugänglich. Besteht das Ziel der Vernetzung hingegen darin, die grenzüberschreitende Zusammenarbeit zwischen den zuständigen Behörden zu Zwecken der Strafverfolgung oder der öffentlichen Verwaltung zu verbessern, z. B. im Fall von ECRIS oder des Prüm-Dienstes von EUCARIS[22], ist der Zugang beschränkt.

Die BRIS-Funktion „Unternehmenssuche“ ist über das Europäische Justizportal für jedermann zugänglich, während die Nachrichten-Infrastruktur derzeit gesetzlich auf nationale Unternehmensregister beschränkt ist. Bei IRI sind die über die Suchschnittstelle erhältlichen Informationen öffentlich zugänglich. Die Mitgliedstaaten können den Zugang nur bei „Verbraucherinsolvenzverfahren“ auf Anforderer mit berechtigtem Interesse beschränken. ECRIS ist nur für die benannten Zentralbehörden der Mitgliedstaaten zugänglich. Ebenso ist der Zugang zu den Diensten von EUCARIS für Behörden nur über die benannten nationalen Kontaktstellen möglich. Der Zugang zu EBOCS ist auf die teilnehmenden Stellen zur Verbrechensbekämpfung beschränkt.

System	Öffentlicher Zugang	Beschränkter Zugang	Anmerkungen
BRIS	Ja		Die BRIS-Funktion „Unternehmenssuche“ ist über das Europäische Justizportal für jedermann zugänglich, während die Nachrichten-Infrastruktur derzeit gesetzlich auf nationale Unternehmensregister beschränkt ist.
IRI	Ja		
ECRIS		Ja	für zentrale Behörden der Mitgliedstaaten, die eigens für diese Aufgabe benannt wurden
EUCARIS		Ja	für die nationalen Kontaktstellen des EUCARIS, über die Behörden je nach Rechtsgrundlage der Zusammenarbeit Zugang erhalten können
EBOCS		Ja	für die an dem Projekt teilnehmenden Stellen zur Verbrechensbekämpfung
LRI	Ja*		erweiterte Funktionen stehen nur authentifizierten Angehörigen von rechtsberatenden Berufen zur Verfügung

Tabelle 1: Zugang der Nutzer zu dem System, das mit dem vernetzten IT-System interagiert

[21] Das „e-Evidence Digital Exchange System“ wurde im Anschluss an die Schlussfolgerungen des Rates vom 9. Juni 2016 zur Verbesserung der Strafjustiz im Cyberspace eingeführt.

[22] Der Zugang zu EUCARIS steht einer ganzen Reihe von Behörden offen. Auf den Prüm-Dienst von EUCARIS dürfen jedoch nur Strafverfolgungsbehörden zugreifen.

* noch nicht betriebsbereit

Die zentralen Mechanismen für Bankkonten sollen im Rahmen der Geldwäscherichtlinie den Kampf gegen Geldwäsche und Terrorismusfinanzierung unterstützen, wobei der Zugang bestimmten Behörden vorbehalten ist. Die Informationen aus den zentralen Mechanismen werden nun, gemäß der Richtlinie zur Erleichterung des Zugangs zu Finanz- und sonstigen Informationen, zusätzlich zur Bekämpfung schwerer Straftaten genutzt; im Rahmen dieser Richtlinie erhalten die benannten zuständigen Behörden ebenfalls Zugangsrechte. Welche Inlandsbehörden jedoch direkten Zugang zu den nationalen Registern erhalten, entscheiden die Mitgliedstaaten, die diese Register führen. Dies könnte zu einem uneinheitlichen Vorgehen führen, da bestimmte Arten von Behörden so in einem Mitgliedstaat Zugang erhalten könnten, in einem anderen jedoch nicht. Bei einem grenzüberschreitenden Austausch über das EU-weite Vernetzungssystem könnte dies zur Folge haben, dass eine Behörde Informationen aus dem Register eines anderen Mitgliedstaats anfordert, während diese Anfrage einer anderen Behörde verweigert wird.

Eine mögliche Lösung dieses Problems wäre, dass die Behörden, die gemäß der Geldwäscherichtlinie und der Richtlinie über die Erleichterung des Zugangs zu Finanz- und anderen Informationen direkten Zugang zu den zentralen Mechanismen haben, auch einen Zugang zur Vernetzungsplattform erhalten. Eine andere Möglichkeit wäre, die Zugangsrechte für das Verbundsystem den gleichen Behörden in allen Mitgliedstaaten zu gewähren, was durch eine auf EU-Ebene harmonisierte, geschlossene Liste der Arten von Behörden erreicht werden könnte, die im Einklang mit dem Zugangszweck festgelegt werden.

Falls die Vernetzung auf alle Behörden ausgeweitet wird, denen derzeit nach nationalen Rechtsvorschriften Zugang gewährt wird, sollten detaillierte Bestimmungen über die Zugangs- und Abfragebedingungen für die zuständigen nationalen Behörden festgelegt werden. In diesem Zusammenhang muss darauf hingewiesen werden, dass die Richtlinie über die Verwendung von Finanz- und anderen Informationen strenge Bedingungen für den Zugang und die Abfrage von – in den zentralen automatischen Mechanismen eingebundenen – Bankkonteninformationen durch die auf nationaler Ebene benannten zuständigen Behörden vorsieht. Zu diesen Bedingungen zählt beispielsweise, dass der Zugang zu den Registern und Datenabrufsystemen auf eigens von den zuständigen Behörden benannte und befugte Personen beschränkt ist. Eine weitere mögliche Maßnahme zur Reduzierung der Risiken, die durch die erweiterten Zugangsrechte der benannten nationalen Behörden entstehen, wäre die Beschränkung der verfügbaren Informationen im Verbundsystem auf die Mindestinformationen zu den Kontenprofilen gemäß Artikel 32a Absatz 3 der Geldwäscherichtlinie.

Artikel 32a Absatz 3 der Geldwäscherichtlinie legt fest, welche Informationen in allen zentralen Systemen erfasst sein müssen, wie etwa der Kontoinhaber, durch die IBAN identifizierte Bankkonten sowie Schließfächer in Kreditinstituten innerhalb des nationalen Hoheitsgebiets. Allerdings sieht Artikel 32a Absatz 4 der Richtlinie die Möglichkeit vor, dass die Mitgliedstaaten weitere Informationen in die Register mitaufnehmen, die von den zentralen Meldestellen und den zuständigen Behörden für die Erfüllung ihrer Pflichten im Rahmen dieser Richtlinie als wesentlich angesehen werden. Aus datenschutzrechtlicher Sicht erscheint es jedoch notwendig, den Umfang der Informationen, die über die Vernetzungsplattform zugänglich sind, auf die Mindestangaben in Artikel 32a Absatz 3 der Geldwäscherichtlinie zu beschränken. Der Zugang zu personenbezogenen Daten sollte im Einklang mit den Datenschutzvorschriften in einem angemessenen Verhältnis zu dem stehen, was zur Erreichung der in der Geldwäscherichtlinie festgelegten Ziele notwendig ist. Ähnlich geht die Richtlinie zur Nutzung von Finanz- und sonstigen Informationen vor. In Artikel 4 Absatz 2 dieser Richtlinie wird klargestellt, dass die zuständigen Behörden keinen Zugang zu den zusätzlichen

Informationen haben, die die Mitgliedstaaten in die zentralen Mechanismen aufnehmen, und diese nicht abfragen können.

3.2. Suchfunktion

Um dem Nutzer durch die Vernetzung der automatisierten zentralen Mechanismen einen Mehrwert bieten zu können, sind die anwendbaren Suchkriterien von entscheidender Bedeutung. Die Suchkriterien sollten so konzipiert sein, dass die zuständigen Behörden ihre Aufgaben erfüllen und Ermittlungen effizienter durchführen können bei gleichzeitiger Wahrung der Verhältnismäßigkeit und der geltenden Datenschutzvorschriften.

Dabei ist zu erwägen, wer zur Abfrage berechtigt sein sollte (private oder öffentliche Akteure) und welche Daten bei der Abfrage als bekannt vorausgesetzt werden können und welche nicht. Sollen zu den Suchkriterien beispielsweise Daten gehören, die demjenigen, der die Suche durchführt, wahrscheinlich nicht bekannt sind, kann eine effektive Abfrage erschwert oder unmöglich werden. Ferner wird darauf hingewiesen, dass es Fälle gibt, in denen einer zentralen Meldestelle oder Strafverfolgungsbehörde eines Mitgliedstaats das Geburtsdatum oder die nationale Identifikationsnummer eines Bürgers eines anderen Mitgliedstaats nicht bekannt ist. Kann jedoch über die Schnittstellen auf solche zusätzlichen Informationen in den zentralen Systemen zugegriffen werden, stellt sich die Frage, ob anhand dieser zusätzlichen Informationen auch Abfragen möglich sein sollen.

Als Suchkriterien könnten die Arten von Angaben ins Auge gefasst werden, die zu den Mindestinformationen gemäß Artikel 32a Absatz 3 der Geldwäscherichtlinie gehören. Damit wäre der ursprüngliche Zweck der zentralen Mechanismen auch im Verbundsystem gewahrt. Zur Verifizierung von Treffern (insbesondere in Fällen, in denen eine Abfrage mehrere Antworten ergibt) wären zusätzliche Sicherungsmaßnahmen erforderlich.

Die anwendbaren Suchmodalitäten sind entscheidend dafür, wie effektiv die vernetzten Datenbanken genutzt werden können. „Fuzzy-Abfragen“, d. h. Abfragen, die eine größere Anzahl an Ergebnissen liefern, auch wenn ein Wort falsch geschrieben oder unvollständig ist, erhöhen die Anzahl der Treffer und damit die Wahrscheinlichkeit, dass die gesuchten Informationen gefunden werden. Allerdings könnte dies aus datenschutzrechtlicher Sicht bedenklich sein, da diese Art der Abfrage personenbezogene Daten offenlegen könnte, die eigentlich nicht anvisiert waren. Eine „genaue Treffer“-Suche hingegen vermindert zwar das Risiko einer unnötigen Offenlegung personenbezogener Daten, erhöht jedoch die Wahrscheinlichkeit, dass die angefragten Informationen von der Suchmaschine übersehen werden (z. B. aufgrund unterschiedlicher Schreibweisen des Eintrags oder der Anwendung unterschiedlicher Transliterationsregeln).

Die Möglichkeit, „Fuzzy-Abfragen“ durchzuführen, würde den Einsatz automatischer Validierungsverfahren verringern und somit die falschen Treffer vermeiden bzw. ihre Anzahl reduzieren, gleichzeitig aber auch den operativen Nutzen des Systems schmälern. Wenn „Fuzzy-Abfragen“ durchgeführt werden, sollten andere Instrumente zur Minderung des Ausforschungsrisikos („fishing expeditions“) in Betracht gezogen werden, wie beispielsweise beim IRI, bei dem die Zahl der angezeigten Ergebnisse begrenzt ist.

3.3. Verwaltungsstruktur, Zuständigkeit für die Wartung

Im Falle von BRIS, IRI, LRI und ECRIS sind die Dienststellen der Europäischen Kommission *für die Wartung des IT-Systems verantwortlich,* d. h. sie müssen die Verfügbarkeit der

Vernetzungskomponente sicherstellen und die Kosten für die Einrichtung und Pflege des Systems tragen. Derzeit wird e-CODEX von einem Konsortium aus Mitgliedstaaten gewartet (die CEF-Komponente „eDelivery“ liegt im Zuständigkeitsbereich der Europäischen Kommission). Die Zuständigkeit für EUCARIS liegt bei den 28 Mitgliedstaaten sowie den beteiligten Drittstaaten, während das System bei EBOCS Eigentum der „European Business Registers'Association“ (Europäischer Verband der Unternehmensregister, EBRA) ist. Für die Wartung sowie die Gewährleistung der Verfügbarkeit der nationalen Datenbanken, die durch diese IT-Systeme vernetzt werden, sind die Mitgliedstaaten zuständig.

In Bezug auf die *Verwaltungsstruktur* eines Systems zur Vernetzung von Datenbanken sollte die Zuständigkeit für Entscheidungen in strategischen und operativen Fragen so gestaltet sein, dass sie den Interessen der nationalen Komponenten gerecht wird.

Bei BRIS fungiert der BRIS-Lenkungsausschuss als internes Forum der Kommission für strategische Entscheidungen sowie für die Beaufsichtigung und Verwaltung von BRIS, während die Gruppe der Gesellschaftsrechtsexperten – Unternehmensregister (CLEG-BRIS) als Forum für die politische Zusammenarbeit zwischen den beteiligten Akteuren fungiert. Eine ähnliche Trennung von politischen und operativen Strukturen lässt sich in Bezug auf EUCARIS beobachten, bei dem die Generalversammlung, die aus hochrangigen Vertretern der Regierungsstellen besteht, die zu verfolgende Strategie festlegt, den Haushalt und die jährlichen Beiträge billigt und Vorkehrungen für die Systemverwaltung trifft.

3.4. Datenaufsicht

Es ist zwischen der Verantwortung für die Wartung des IT-Systems und der *Verantwortung aus datenschutzrechtlicher Sicht* zu unterscheiden. Nach der Datenschutz-Grundverordnung[23] ist der Verantwortliche die natürliche oder juristische Person, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet und die Verantwortung für die Verarbeitung personenbezogener Daten trägt. Das Problem der Zuständigkeit ist komplex; bei der Bestimmung des Verantwortlichen spielen viele Faktoren eine Rolle, u. a. die Frage, wer die Daten speichert und wo.

Bei IRI dient die EU-Plattform lediglich der Vernetzung der dezentralen nationalen Datenbanken; alle Daten, die in der zentralen Plattform angezeigt werden, sind lediglich „vorübergehende Daten“ – sie werden also weder in der EU-Komponente gespeichert, noch werden Abfrage-Protokolle erstellt oder gespeichert. Anders gestaltet sich die Situation bei BRIS – hier wurde eine spezielle Funktion eingeführt, die die Kernprofildaten der Unternehmen in einer zentralen Komponente auf Kommissionsebene speichert, die regelmäßig von den nationalen Registern aktualisiert wird. Die erste Abfrage erfolgt in dieser zentralen Datenbank und ergibt eine Trefferliste mit den Namen der Einrichtungen. Der Anforderer erhält detaillierte Daten zu einer bestimmten Einrichtung, indem er den Namen dieser Einrichtung aus der Trefferliste auswählt; so wird eine direkte Verknüpfung zu den Informationen in der nationalen Datenbank hergestellt.

Hinsichtlich einer möglichen Vernetzung zentraler Mechanismen sollte die Entwicklung eines IT-Systems in Erwägung gezogen werden, bei dem die zentrale Routing-Komponente keine personenbezogenen Daten speichert und alle Entscheidungen über die Mittel und Zwecke der

[23]Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016.

Datenverarbeitung auf nationaler Ebene getroffen werden. Ziel des Vernetzungsdienstes wäre lediglich, die Datenverarbeitung für die zentralen Mechanismen, die für ihre Datensätze selbst verantwortlich blieben, zu erleichtern.

3.5. Einrichtungs- und Wartungskosten

Die Einrichtung eines Systems, das die nationalen zentralen Mechanismen miteinander vernetzt, wird mit Kosten verbunden sein, die sowohl durch die Einrichtung als auch durch die Wartung des Systems entstehen, wobei die Kosten zwischen der EU und den Mitgliedstaaten aufgeteilt werden müssten. Betrachtet man die Kostenaufteilung in den Modellbeispielen, so wurden in der Regel die Kosten im Zusammenhang mit der EU-Komponente (Komponente, EU-Plattform) aus dem Gesamthaushaltsplan der EU finanziert, während die Mitgliedstaaten die Kosten für die Anpassung der nationalen Systeme und deren Interoperabilität mit dem System der EU trugen. Im Falle des BRIS kostete die Entwicklung der ersten Version, die im Juni 2017 in Betrieb genommen wurde, einschließlich der zentralen Europäischen Plattform rund 1,7 Mio. EUR. Beim IRI, das eine einfachere Architektur aufweist, beliefen sich die Kosten für die Entwicklung der ersten Version des zentralen Suchsystems (IRI 1.0) auf etwa 280 000 EUR, während die Anpassung der zentralen Suchanwendung bei IRI 2.0 etwa 170 000 EUR kosten wird. Beim ECRIS beliefen sich die Gesamtkosten für den Einsatz der „Referenzimplementierung“, also der Software für den Austausch von Strafregisterdaten zwischen den Mitgliedstaaten, auf 2 050 000 EUR. Die jährlichen Kosten für die Wartung des Systems beliefen sich auf 150 000 EUR. Für EUCARIS zahlt jedes teilnehmende Land eine allgemeine Wartungsgebühr in Höhe von 20 000 EUR.

Betrachtet man die vorstehenden Zahlen, so wird klar, dass die Kosten für die Einrichtung und Wartung eines EU-weiten Vernetzungssystems im Vergleich zu den Vorteilen, die ein solches Projekt für die EU mit sich bringt, relativ niedrig sind. Die Kosteneffizienz ließe sich durch die Verwendung bereits vorhandener Kapazitäten (wie z. B. Zugangspunkte von eDelivery, Bausteine der Fazilität „Connecting Europe“, Kernvokabulare der Generaldirektion Informatik der Europäischen Kommission usw.) verbessern.

4. Technische Spezifikationen der Systeme, einschließlich Datensicherheit

4.1. Verwendetes Netzwerk und Datensicherheit

Der Prüm-Dienst von EUCARIS und ECRIS nutzt die transeuropäischen Telematikdienste für Behörden (TESTA) – ein privates Netzwerk, das vollständig vom öffentlichen Internet getrennt ist. Die benannten nationalen Kontaktstellen haben Zugang zu diesem privaten Netzwerk. Der TESTA-Netzwerkdienst wird von der Kommission betrieben und bietet eine Leistungsgarantie und ein hohes Maß an Sicherheit. Was EUCARIS betrifft, so kann das System über das öffentliche Internet benutzt werden, was derzeit jedoch nicht getan wird. Es ist mit allen EU-Institutionen und nationalen Netzwerken verbunden und wird im Rahmen der Zusammenarbeit bei der Strafverfolgung, die sensible Informationen umfasst, bevorzugt. Die EU-Institutionen haben noch weitere sichere Netzwerke entwickelt, wie z. B. das Gemeinsame Kommunikationsnetz/die Gemeinsame Systemschnittstelle (CCN/CSI), die in den Bereichen Zollpolitik und Besteuerung eingesetzt werden.

BRIS, IRI, LRI und EBOCS nutzen das öffentliche Internet (mit einer geeigneten Verschlüsselungstechnik für Daten, die über das Internet ausgetauscht werden). Was den sicheren Informationsaustausch über das öffentliche Internet betrifft, so können Unternehmen und öffentliche Verwaltungen dank des eDelivery-Bausteins auf interoperable, sichere, zuverlässige und

vertrauenswürdige Weise elektronische Daten und Dokumente in digitaler Form mit anderen Organisationen austauschen. Dies steht im Einklang mit der Definition der Dienste für die Zustellung elektronischer Einschreiben („ERDS“) in Artikel 3 Nummer 36 der eIDAS-Verordnung.[24]

Für die mögliche Vernetzung zentraler Systeme mit sensiblen Informationen könnte die Anwendung von TESTA erwogen werden. Aber auch Internet-Lösungen könnten infrage kommen. Fast alle nationalen zentralen Systeme nutzen das öffentliche Internet. Was Datensicherheit und -integrität betrifft, so wird die Tatsache, dass das System aus dezentralen Datenbanken bestehen wird, zu einer Reduzierung der möglichen Risiken beitragen. Dies ist darauf zurückzuführen, dass die Dezentralisierung und eine Aufteilung auf verschiedene Technologien *per se* einen besseren Schutz gegen Cyberangriffe gewährleisten, da sich dadurch eine allgemeine Beschädigung von Daten sehr viel schwieriger und die Wiederherstellung von Daten nach Zwischenfällen wesentlich leichter gestaltet.

4.2. Zentrale Routing-Komponente

In Bezug auf die Struktur von IT-Systemen gibt es zwei wesentliche Architektur-Typen: die völlig dezentralen Systeme und die Systeme, die über eine zentrale Plattform oder Routing-Komponente auf EU-Ebene verfügen, die als Verbindungsglied zwischen den dezentralen nationalen Datenbanken fungiert.

Bei „rein verteilten Systemen“ gibt es keine EU-Plattform oder - Komponente; in diesen Fällen kommunizieren alle Länder direkt miteinander und verfügen dabei über gemeinsam vereinbarte Standards, die einen direkten Peer-to-Peer-Austausch zwischen den angeschlossenen Stellen der Mitgliedstaaten ermöglichen. Abfragen werden daher einzeln an alle anderen nationalen Systeme versendet, und die erhaltenen Antworten werden über die Oberfläche des Web-Client des Anforderers gesammelt und angezeigt. Diese Technologie wird bei EUCARIS, ECRIS und e-CODEX genutzt (basierend auf einer gemeinsam entwickelten Anwendung).

In „verteilten Systemen mit einer zentralen Leitwegkomponente“ gibt es eine zentrale Plattform auf EU-Ebene: Dabei handelt es sich um einen einzelnen zentralen Webdienst, der auf EU-Ebene gewartet und betrieben wird und der mit allen nationalen Systemen vernetzt ist. Nutzer führen die Abfragen über diesen zentralen Webdienst durch, der die Informationen aus den nationalen Datenbanken sammelt. Diese Technologie wird bei BRIS, EBOCS und IRI angewandt.[25]

Hinsichtlich der Konnektivität wäre eine Lösung mit einer zentralen Routing-Komponente einfacher in der Umsetzung. Wenn es nur eine einzige Plattform gäbe, müsste jeder Mitgliedstaat nur eine Verbindung zwischen dem nationalen System und dieser zentralen Plattform herstellen und warten. Fehlt jedoch eine solche „echte“ zentrale Plattform, muss jeder Mitgliedstaat Verbindungen zu allen anderen nationalen Systemen der Mitgliedstaaten herstellen, testen und warten (z. B. zählt der Prüm-Dienst von EUCARIS derzeit fast 756 Verbindungen). Diese Vielzahl an Anschlüssen stellt eine

[24] Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (ABl. L 257 vom 28.8.2014, S. 73).

[25] Es gibt Alternativen zu einer zentralen Komponente. So können beispielsweise die Teilnehmer einer Nachrichten-Infrastruktur über den eDelivery-Dienst „Service Metadata Publisher“ (SMP) der CEF die jeweiligen (rechtlichen, organisatorischen und technischen) Möglichkeiten der anderen dynamisch entdecken. Aufgrund dieser verteilten Architektur muss jeder Teilnehmer über eine eindeutige ID verfügen. Eine zentrale Komponente, nämlich „Service Metadata Locator“ (SML), verwendet diese IDs zur Erstellung von URLs, die, wenn sie aufgelöst werden, die Zugangspunkte von eDelivery zu den spezifischen Informationen über den Teilnehmer lenken.

Herausforderung dar, die die Probleme in Bezug auf Steuerung, Kontrolle und Prüfung vergrößern kann; ein rein verteiltes System müsste dieser Herausforderung gerecht werden. Es gibt aber durchaus technologische Lösungen für die Bewältigung der großen Zahl möglicher Verbindungen. Gleichzeitig muss jedoch auch die Tatsache angemessen berücksichtigt werden, dass sich die zentrale Komponente in einem zentralen Routing-System zu einem Single Point of Failure (SPoF) im Gesamtsystem entwickeln kann.

4.3. Datenaustauschprotokoll

Das BRIS und e-CODEX verwenden die eDelivery-Lösung der CEF, während bei IRI 2.0 sowohl die Kommunikation mit CEF eDelivery als auch mit SOAP[26] genutzt wird. Der Prüm-Dienst von EUCARIS und die EBOCS nutzen die SOAP-basierten Schnittstellen. LRI verwendet die REStful-Webdienste[27].

Mit dem eDelivery-Baustein der CEF können Nutzer untereinander auf sichere, zuverlässige und vertrauenswürdige Weise elektronische Daten austauschen. Die eDelivery-Lösung der CEF stützt sich auf ein verteiltes Modell mit der Bezeichnung „4-corner model", bei dem die Backend-Systeme der Nutzer Daten nicht direkt, sondern über Zugangspunkte austauschen. Diese Zugangspunkte weisen die gleichen technischen Spezifikationen auf und können daher miteinander kommunizieren. Ein weiterer Vorteil von eDelivery ist, dass der Datenaustausch zwischen den verschiedenen Zugangspunkten sicher erfolgen kann, ohne dass eine maßgeschneiderte Lösung erforderlich ist. Daher können Nutzer, die CEF eDelivery anwenden, problemlos und sicher Daten austauschen, selbst wenn ihre IT-Systeme unabhängig voneinander entwickelt wurden. Ebenso können durch das eDelivery-Model, das für die Verknüpfung verschiedener Backend-Systeme sehr nützlich ist, verschiedene Funktionen zentralisiert werden. Wenn diese Technologie verwendet wird, müssen die Mitgliedstaaten (und gegebenenfalls die Kommission, falls es sich um eine zentrale Routing-Komponente handelt) ein eDelivery-Gateway auf ihrer jeweiligen Ebene einrichten. Sie können dafür ihre bereits existierenden, für andere Dienste entwickelten Gateways verwenden (was zur Kosteneffizienz der Lösung beiträgt). Die Generaldirektion Informatik der Europäischen Kommission hat eine kompatible Softwarelösung entwickelt, die sie mit einer Open-Source-Lizenz für die Europäische Union (EUPL) kostenlos zur Verfügung stellt. Dabei sind in der Regel jedoch noch gewisse bedarfsorientierte Anpassungen und Entwicklungen erforderlich. Das eDelivery-Model folgt einer asynchronen Kommunikation, die implizit gewisse Latenzen bei der Leistung verursacht (in der Regel 3-10 Sekunden). Hinsichtlich der Bausteine der CEF verfolgt die EU im Allgemeinen eine Politik, die auf eine Konvergenz der verschiedenen Systeme, die in den unterschiedlichen Politikbereichen der EU entwickelt wurden, abzielt.

In den Fällen, in denen ein synchrones SOAP eingesetzt wird – was die Kommunikation über eine gesicherte Schicht ermöglicht –, wird meist eine einfachere Architektur gewählt, die auf optimale Leistung abzielt. Eine neuere Lösung im Vergleich zu SOAP ist der RESTful-Architekturstil – es ist bereits absehbar, dass die REST-Technologie SOAP verdrängen wird. Den eDelivery- sowie den SOAP- oder REST-basierten Ansätzen ist gemein, dass sich das Vertrauen in der Regel auf elektronische Zertifikate stützt und verschiedene Kontrollen durchgeführt werden.

In Bezug auf die künftige Vernetzung der zentralen Mechanismen wird darauf hingewiesen, dass CEF eDelivery dann verwendet wird, wenn der bilaterale Austausch zwischen den dezentralen nationalen

[26] „Simple Object Access Protocol".
[27] „Representational State Transfer" ist eine Art der Software-Architektur, die eine Reihe von Einschränkungen für die Erstellung von Web-Diensten definiert.

Datenbanken stattfindet. Bei Systemen, bei denen die Kommunikation nur zwischen einer nationalen Datenbank und der zentralen Plattform stattfindet, reicht hingegen die SOAP-basierte Schnittstelle (oder RESTful) aus.

4.4. Arbeit in einer mehrsprachigen Umgebung und semantische Interoperabilität

Alle bewerteten Systeme arbeiten in einer mehrsprachigen Umgebung. EBOCS, bildet mit derzeit nur drei Sprachen eine Ausnahme, soll jedoch langfristig in allen Sprachen arbeiten. Bei BRIS erfolgt die Transliteration auf EU-Ebene, während sie bei IRI, LRI und EUCARIS auf nationaler Ebene stattfindet. In Bezug auf semantische Interoperabilität (Glossare) erfordert eine künftige Vernetzung zentraler Mechanismen kein spezifisches Vokabular, da die Mindestauswahl an Informationen nicht aus nationalen Begriffen, sondern aus personenbezogenen Daten wie Name, eindeutige Kennung (z. B. nationale ID-Nummern) und IBAN-Nummer besteht. Bei allen nationalen Systemen ist ein gemeinsames Verständnis von entscheidender Bedeutung, insbesondere weil die nationalen zentralen Mechanismen keine Informationen über Einrichtungen der EU und von Drittländern enthalten. Zu diesem Zweck könnten die Transliterationsregeln des Schengener Informationssystems (SIS) als nützliche Vorlage dienen.

Gemäß dem Europäischen Interoperabilitätsrahmen (EIF) bezieht sich der semantische Aspekt auf die Bedeutung von Datenelementen und ihre Beziehungen untereinander. Dies schließt die Entwicklung von Vokabularen und Schemata zur Beschreibung des Datenaustauschs mit ein und stellt sicher, dass Datenelemente von allen kommunizierenden Parteien in gleicher Weise verstanden werden.

Das System zur Vernetzung von Bankenregistern muss Daten zwischen verschiedenen Datenbanken austauschen, wobei jede Datenbank eigene Datenmodelle und semantische Standards hat. Dabei müssen gemeinsame semantische Standards entweder nativ in den Systemen oder als Mapping-Schicht zwischen den verschiedenen Standards in den Mitgliedstaaten festgelegt werden. Vor der Entwicklung eines neuen semantischen Standards ist jedoch die Anwendung bereits bestehender Standards in Erwägung zu ziehen.

Bei den Kernvokabularen (Unternehmen, Ort, Person und weitere), die vom Programm ISA2 erstellt werden, handelt es sich um vereinfachte, wiederverwendbare und erweiterbare Datenmodelle, die zu diesem Zweck verwendet werden können. Die unterschiedlichen Lösungen für die Vernetzung von Basisregistern (z. B. BRIS) nutzen bereits einige der Standards, z. B. das Core Business Vocabulary (CBS).

5. Nächste Schritte

Dieser Bericht beschreibt einige Elemente, die bei einer Vernetzung von Bankkontenregistern und Datenabrufsystemen zu berücksichtigen sind, und macht deutlich, dass die Vernetzung solcher zentraler Mechanismen technisch machbar ist. Die Umsetzung könnte z. B. in Form eines dezentralen Systems mit einer gemeinsamen Plattform auf EU-Ebene erfolgen. Dazu könnte man auf Technologien zurückgreifen, die die Europäische Kommission bereits im Rahmen der verschiedenen analysierten Modelle entwickelt hat.

In den letzten Jahren wurden die gemeinsamen Bausteine in verschiedenen Systemen wiederverwendet. Bei diesen Bausteinen handelt es sich im Wesentlichen um eine Auswahl an bekannten Standards und technischen Spezifikationen, mit denen wiederkehrende Herausforderungen wie der sichere Informationsaustausch bewältigt werden können. Der konsequente Rückgriff auf diese Bausteine wird von der Kommission in ihrer aktuellen Digitalpolitik befürwortet und von den

Mitgliedstaaten in der Erklärung von Tallinn zu elektronischen Behördendiensten[28] unterstützt. Der Rückgriff auf diese Bausteine könnte die zukünftige Vernetzung nationaler zentraler automatischer Mechanismen und ihre Anpassung an einschlägige EU-Vorschriften wie eIDAS beschleunigen.

Eine künftige EU-weite Vernetzung der zentralen Mechanismen würde den Zugang zu Finanzinformationen beschleunigen und die grenzüberschreitende Zusammenarbeit der zuständigen Behörden erleichtern. Die Kommission beabsichtigt daher, weitere Konsultationen mit den relevanten Interessenträgern, den Regierungen sowie den zentralen Meldestellen, Strafverfolgungsbehörden und Vermögensabschöpfungsstellen als potenzielle „Endnutzer“ eines möglichen Vernetzungssystems durchzuführen.

[28]Alle Mitgliedstaaten der Europäischen Union und die EFTA-Länder haben am 6. Oktober 2017 in Tallinn die „eGovernment-Erklärung“ unterzeichnet. Der Text der Erklärung ist auf folgender Website (auf Englisch) abrufbar: http://ec.europa.eu/newsroom/document.cfm?doc_id=47559.