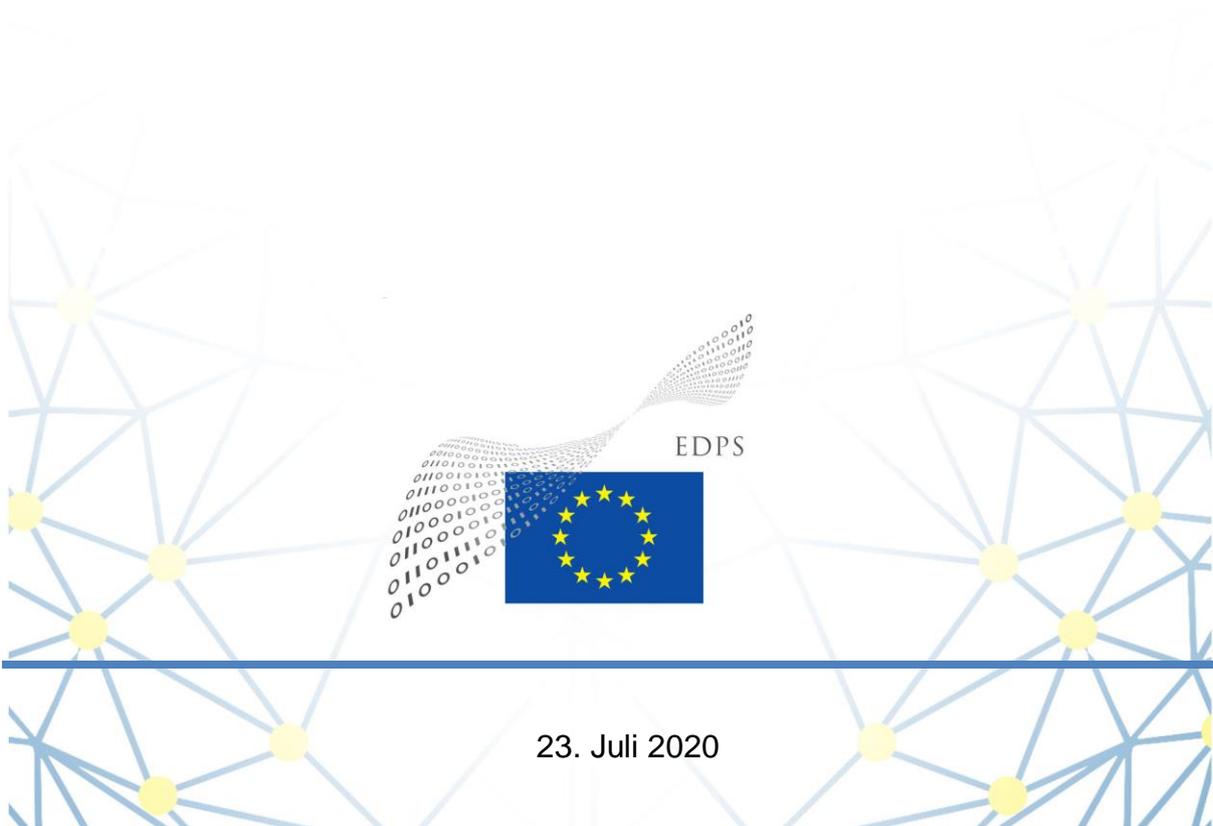


EUROPEAN DATA PROTECTION SUPERVISOR

# Stellungnahme 5/2020

**zum Aktionsplan der Europäischen  
Kommission für eine umfassende  
Politik der Union zur Verhinderung von  
Geldwäsche und  
Terrorismusfinanzierung**



23. Juli 2020

*Der Europäische Datenschutzbeauftragte (EDSB) ist eine unabhängige Behörde der EU und hat nach Artikel 52 Absatz 2 der Verordnung (EU) 2018/1725 im „Hinblick auf die Verarbeitung personenbezogener Daten ... sicherzustellen, dass die Grundrechte und Grundfreiheiten natürlicher Personen, insbesondere ihr Recht auf Datenschutz, von den Organen und Einrichtungen der Union geachtet werden“; gemäß Artikel 52 Absatz 3 ist er „für die Beratung der Organe und Einrichtungen der Union und der betroffenen Personen in allen Fragen der Verarbeitung personenbezogener Daten“ zuständig. Nach Artikel 58 Absatz 3 Buchstabe c der Verordnung 2018/1725 hat der EDSB die Befugnis, „zu allen Fragen, die im Zusammenhang mit dem Schutz personenbezogener Daten stehen, von sich aus oder auf Anfrage Stellungnahmen an die Organe und Einrichtungen der Union sowie an die Öffentlichkeit zu richten“.*

*Am 5. Dezember 2019 wurde Wojciech Wiewiorowski für einen Zeitraum von fünf Jahren zum Europäischen Datenschutzbeauftragten ernannt.*

## Zusammenfassung

**In der am 7. Mai 2020 von der Kommission vorgelegten Mitteilung zu einem Aktionsplan für eine umfassende Politik der Union zur Verhinderung von Geldwäsche und Terrorismusfinanzierung (C(2020)2800 final) ist der Fahrplan zur Erreichung der Ziele in diesem Bereich festgelegt. Diese Stellungnahme bewertet die den Datenschutz betreffenden Implikationen der im Aktionsplan der Kommission vorgesehenen Initiativen.**

**Der EDSB erkennt an, dass die Bekämpfung von Geldwäsche und Terrorismusfinanzierung als Ziel von allgemeinem Interesse einen hohen Stellenwert hat, hält es jedoch für wichtig, dass beim Erlass der einschlägigen Rechtsvorschriften auf ein angemessenes Gleichgewicht zwischen dem Eingriff in die Grundrechte auf den Schutz der Privatsphäre und der personenbezogenen Daten und den erforderlichen Maßnahmen zur wirksamen Erreichung der im Allgemeininteresse liegenden Ziele im Bereich der Bekämpfung von Geldwäsche und Terrorismusfinanzierung (im Folgenden auch: AML/CFT) geachtet wird (Verhältnismäßigkeitsgrundsatz).**

**Der EDSB empfiehlt der Kommission, im Zuge der Überwachung der tatsächlichen Umsetzung des bestehenden Rahmens für die Bekämpfung von Geldwäsche und Terrorismusfinanzierung die Wahrung und Einhaltung der Datenschutz-Grundverordnung (DSGVO) und des Datenschutzrahmens sicherzustellen. Von besonderer Relevanz ist dies für die Arbeiten an der Vernetzung der zentralen Bankkontenmechanismen und der Register wirtschaftlicher Eigentümer, die vor allem den Grundsätzen der Datenminimierung, der Richtigkeit sowie des Datenschutzes durch Technikgestaltung und datenschutzfreundliche Voreinstellungen Rechnung tragen sollten.**

**Der EDSB begrüßt die vorgesehene Harmonisierung des Rahmens für die Bekämpfung von Geldwäsche und Terrorismusfinanzierung, da diese zu einer einheitlicheren Anwendung der Hauptvorschriften in den Mitgliedstaaten sowie zu einer einheitlichen Auslegung durch den Gerichtshof der Europäischen Union führen wird. Der EDSB fordert die Kommission auf, bei der Entscheidung über die im verbesserten Regelwerk vorgesehenen Maßnahmen dem risikobasierten Ansatz zu folgen, da dieser Ansatz auch mit den Datenschutzgrundsätzen in Einklang steht.**

**Der EDSB empfiehlt der Kommission, in ihrem Vorschlag für die Einführung einer auf EU-Ebene angesiedelten Aufsicht über die Bekämpfung von Geldwäsche und Terrorismusfinanzierung eine spezifische Rechtsgrundlage für die Verarbeitung personenbezogener Daten sowie die nach der DSGVO und der Verordnung (EU) 2018/1725 erforderlichen Datenschutzgarantien vorzusehen, insbesondere in Bezug auf den Informationsaustausch und internationale Datenübermittlungen.**

**Der EDSB begrüßt die Initiative der Kommission, den Ausbau von FIU.net zu fördern und eine geeignete Lösung für dessen Verwaltung zu finden, die mit der DSGVO und dem Datenschutzrahmen in Einklang steht. Des Weiteren empfehlen wir, im Vorschlag zur Einrichtung eines EU-Koordinierungs- und -Unterstützungsmechanismus für zentrale Meldestellen die Voraussetzungen klarzustellen, unter denen zentralen Meldestellen der Zugang zu und der Austausch von Informationen über Finanztransaktionen gestattet ist.**

**Der EDSB unterstützt den Aufbau öffentlich-privater Partnerschaften (ÖPP) zur Erforschung und Analyse von Typologien und Trends für die Zwecke der Bekämpfung von Geldwäsche und Terrorismusfinanzierung, sofern die sich aus der DSGVO ergebenden**

**Grenzen eingehalten werden. Allerdings ist der EDSB, ohne eine Beurteilung der der Initiative zugrunde liegenden politischen Zwecke vornehmen zu wollen, der Ansicht, dass ÖPP, in deren Rahmen Strafverfolgungsbehörden operative Informationen über einschlägige Verdächtige an Verpflichtete weitergeben, die Rechte auf den Schutz der Privatsphäre und Datenschutz in hohem Maße gefährden würden. Auch Verarbeitungsvorgänge, die Informationen über etwaige sich aus Finanztransaktionen ergebende Straftaten betreffen, sollten bei den zuständigen Behörden verbleiben und nicht an private Stellen weitergegeben werden.**

**Der EDSB begrüßt die Bemühungen der Kommission, sich stärker in der Financial Action Task Force (FATF) zu engagieren und dort mit einer Stimme zu sprechen. Er regt an, dass sich die Kommission bei der Aufstellung internationaler Standards im Bereich der Bekämpfung von Geldwäsche und Terrorismus (AML/CFT) dafür einsetzt, die Datenschutzgrundsätze als unverzichtbaren Bestandteil in die AML/CFT-Prozesse aufzunehmen.**

**Der EDSB erwartet, nach der Annahme von Vorschlägen für Gesetzgebungsakte, die Auswirkungen auf den Schutz der Rechte und Freiheiten natürlicher Personen bei der Verarbeitung personenbezogener Daten haben, gemäß Artikel 42 der Verordnung (EU) 2018/1725 konsultiert zu werden. Unter anderem betrifft dies auch künftige Vorschläge für eine Verordnung über Maßnahmen zur Bekämpfung von Geldwäsche und Terrorismus, zur Einrichtung eines EU-Unterstützungs- und Kooperationsmechanismus für zentrale Meldestellen und zur Schaffung einer auf EU-Ebene angesiedelten Aufsicht über die Bekämpfung von Geldwäsche und Terrorismusfinanzierung.**

# INHALTSVERZEICHNIS

## Inhalt

1.	EINLEITUNG UND HINTERGRUND .....	6
2.	ALLGEMEINE KOMMENTARE .....	7
2.1	Grundsatz der Verhältnismäßigkeit Angemessenes Gleichgewicht zwischen dem Schutz der personenbezogenen Daten und der Bekämpfung von Geldwäsche und Terrorismusfinanzierung .....	7
3.	ANMERKUNGEN UND EMPFEHLUNGEN.....	8
3.1.	Erste Säule: Gewährleistung der wirksamen Umsetzung des bestehenden EU-Rahmens zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung .....	8
3.2.	Zweite Säule: Schaffung eines verbesserten Regelwerks .....	10
3.3.	Dritte Säule: Einführung einer auf EU-Ebene angesiedelten Aufsicht.....	12
3.4.	Vierte Säule: Einrichtung eines Unterstützungs- und Kooperationsmechanismus für die zentralen Meldestellen .....	13
3.5.	Fünfte Säule: Durchsetzung strafrechtlicher Bestimmungen und Informationsaustausch auf Unionsebene .....	15
3.6.	Sechste Säule: Stärkung der internationalen Dimension des EU-Rahmens.....	18
4.	SCHLUSSFOLGERUNGEN .....	18
	Endnoten .....	19

## **DER EUROPÄISCHE DATENSCHUTZBEAUFTRAGTE –**

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf Artikel 16,

gestützt auf die Charta der Grundrechte der Europäischen Union, insbesondere auf die Artikel 7 und 8,

gestützt auf die 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)<sup>1</sup>,

gestützt auf die Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union und zum freien Datenverkehr<sup>2</sup>, insbesondere auf Artikel 58 Absatz 3 Buchstabe c –

### **HAT FOLGENDE STELLUNGNAHME ANGENOMMEN:**

#### **1. EINLEITUNG UND HINTERGRUND**

1. Am 7. Mai 2020 wurde von der Europäischen Kommission eine Mitteilung zu einem Aktionsplan für eine umfassende Politik der Union zur Verhinderung von Geldwäsche und Terrorismusfinanzierung (C(2020)2800 final) (im Folgenden: Aktionsplan) vorgelegt. Der Aktionsplan ist eine Initiative, die im Arbeitsprogramm 2020 der Kommission für das politische Ziel Nr. 21 „Vollendung der Bankenunion“ vorgesehen ist.
2. Der Aktionsplan umfasst sechs Säulen, nämlich: 1) Gewährleistung der wirksamen Umsetzung des bestehenden EU-Rahmens zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung; 2) Schaffung eines einheitlichen EU-Regelwerks zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung; 3) Einführung einer auf EU-Ebene angesiedelten Aufsicht zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung; 4) Einrichtung eines Unterstützungs- und Kooperationsmechanismus für die zentralen Meldestellen; 5) Durchsetzung strafrechtlicher Bestimmungen und Informationsaustausch auf Unionsebene sowie 6) Stärkung der internationalen Dimension des EU-Rahmens zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung. Parallel zur Annahme des Aktionsplans leitete die Kommission am 7. Mai eine öffentliche Konsultation<sup>3</sup> ein, in der allen Bürgerinnen und Bürger sowie Organisationen bis zum 29. Juli 2020 Gelegenheit gegeben wurde, sich zu den vorgeschlagenen Maßnahmen zu äußern.
3. Im Aktionsplan wird konkret dargelegt, welche Maßnahmen im Rahmen der Säulen ergriffen werden, u. a. die verschiedenen Gesetzesvorhaben für das einheitliche EU-Regelwerk zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung, die Einführung einer auf EU-Ebene angesiedelten Aufsicht über die Bekämpfung von Geldwäsche und Terrorismusfinanzierung sowie die Einrichtung eines Unterstützungs- und Kooperationsmechanismus für die zentralen Meldestellen (Financial Intelligence Units (FIU)). In dieser Stellungnahme, die der an den sechs Säulen orientierten Gliederung folgt, erörtert der EDSB seine Ansichten zu ausgewählten Maßnahmen des Aktionsplans, insbesondere dazu, wie diese möglicherweise in das in den Artikeln 7 und 8 der Charta der Grundrechte der Europäischen Union garantierte Recht auf Privatsphäre und Datenschutz

eingreifen. Diese Stellungnahme lässt die Verpflichtung der Kommission unberührt, den EDSB gemäß Artikel 42 der Verordnung (EU) 2018/1725 bezüglich aller Vorschläge für Gesetzgebungsakte, die gegebenenfalls im Rahmen des Aktionsplans vorgelegt werden und die Auswirkungen auf den Schutz der Rechte und Freiheiten natürlicher Personen bei der Verarbeitung personenbezogener Daten haben, zu konsultieren.

## 2. ALLGEMEINE KOMMENTARE

### 2.1 Grundsatz der Verhältnismäßigkeit Angemessenes Gleichgewicht zwischen dem Schutz der personenbezogenen Daten und der Bekämpfung von Geldwäsche und Terrorismusfinanzierung

4. Der hohe Stellenwert der Aufstellung eines starken Rahmens sowie der Schaffung geeigneter und wirksamer Strukturen, die mit den notwendigen technischen Mitteln zum Ausbau der Aufgabenwahrnehmung im Bereich der Bekämpfung von Geldwäsche und Terrorismusfinanzierung ausgestattet sind, wird vom EDSB anerkannt. Das Erreichen dieser legitimen und wichtigen Ziele darf jedoch nicht auf Kosten des Schutzes der Privatsphäre und der Rechte der natürlichen Personen an ihren personenbezogenen Daten geschehen; diese Rechte behalten ihre volle Geltung. Die Datenschutzerfordernisse sind nämlich als im Rahmen der Verpflichtungen zur Geldwäschebekämpfung einzuhaltende Grundanforderung zu verstehen.
5. Nach der Rechtsprechung des Gerichtshofs der Europäischen Union entspricht die Bekämpfung schwerer Kriminalität einer dem Gemeinwohl dienenden Zielsetzung<sup>4</sup>, die einen solchen Eingriff in die in den Artikeln 7 und 8 der Charta der Grundrechte der Europäischen Union garantierten Rechte auf Privatsphäre und Datenschutz rechtfertigen kann. Allerdings ist der Gestaltungsspielraum des Unionsgesetzgebers eingeschränkt, und der Rechtsakt muss ein Gleichgewicht zwischen dem Eingriff, der auf das absolut Notwendige zu beschränken ist, und dem Recht natürlicher Personen auf den Schutz der Privatsphäre und der personenbezogenen Daten vorsehen (**Verhältnismäßigkeit**). Eingehendere Ausführungen zum Verhältnismäßigkeitsgrundsatz im Rahmen des Datenschutzes sind dem vom EDSB vorgelegten **Toolkit zur Beurteilung der Erforderlichkeit**<sup>5</sup> wie auch den **Leitlinien des EDSB für die Bewertung der Verhältnismäßigkeit von Maßnahmen, die die Grundrechte auf Privatsphäre und den Schutz personenbezogener Daten einschränken**<sup>6</sup>, zu entnehmen.
6. Der gesetzliche Rahmen der EU für die Bekämpfung von Geldwäsche und Terrorismusfinanzierung wurde in den letzten Jahren rapide weiterentwickelt und ausgebaut. Mit der vierten und fünften Geldwäscherichtlinie wurden wichtige Maßnahmen eingeführt, und diese Fortschritte werden mit der bis 2021 umzusetzenden sechsten Geldwäscherichtlinie<sup>7</sup> fortgeführt.<sup>8</sup> Der EDSB begrüßt, dass die sechste Geldwäscherichtlinie wichtige Änderungen bringt, die auf das Recht auf Privatsphäre und den Schutz personenbezogener Daten abgestimmt sind, z. B. die Verpflichtung der Ermittlungs- bzw. Strafverfolgungsbehörden, Ermittlungsinstrumente gezielt einzusetzen, einem risikobasierten Ansatz<sup>9</sup> (wonach bei geringer Gefahrenlage nur geringe Grundrechtseingriffe gestattet sind) zu folgen sowie dem Grundsatz der Verhältnismäßigkeit sowie der Art und Schwere der untersuchten Straftaten Rechnung tragen.<sup>10</sup>
7. Der EDSB hat zu diesen legislativen Entwicklungen Beratung erteilt und in seinen Stellungnahmen aus den Jahren 2013<sup>11</sup> und 2017<sup>12</sup> (im Folgenden: **Stellungnahme von 2013 zum Vorschlag für die vierte Geldwäscherichtlinie** bzw. **Stellungnahme 1/2017**)

Empfehlungen gegeben, die sicherstellen sollten, dass die Datenschutzgarantien in den Vorschlägen für die vierte und die fünfte Geldwäscherichtlinie ordnungsgemäß berücksichtigt werden.

8. Insbesondere in unserer Stellungnahme von 2013 zum Vorschlag für die vierte Geldwäscherichtlinie haben wir darauf bestanden, dass die **Datenschutzgarantien** auch im Zusammenhang mit den Verfahren zur Erfüllung der kundenbezogenen Sorgfaltspflichten (**customer due diligence (CDD)**) zu beachten sind. Es wurde von uns darauf hingewiesen, dass die Datenverarbeitung nach den Geldwäscherichtlinien allein dem Zweck, Geldwäsche und Terrorismusfinanzierung zu verhindern, dienen muss und dass Verpflichtete wie auch staatliche Stellen **die Daten nicht für andere unvereinbare Zwecke** (z. B. zu Geschäfts- oder Marketingzwecken) **weiterverarbeiten dürfen**.
9. Des Weiteren bestanden wir auf die Beachtung der **Grundsätze der Notwendigkeit und Verhältnismäßigkeit bei der Beschränkung der Rechte der betroffenen Personen** bei der Bekanntmachung von Verwaltungssanktionen und empfahlen, Alternativen und weniger einschneidende Optionen als die allgemeine **Bekanntmachung** in Erwägung zu ziehen. Auch der Erlass **materiellrechtlicher Bestimmungen, die eine Auflistung der Identifikationsdaten über wirtschaftlich Berechtigte enthalten**, die von den zentralen Registern wirtschaftlicher Eigentümer verarbeitet werden, wurde von uns für erforderlich gehalten. Diesbezüglich bestimmt jetzt Artikel 30 Absatz 5 der vierten Geldwäscherichtlinie, dass die von diesen Registern verarbeiteten personenbezogenen Daten mindestens den Namen, Monat und Jahr der Geburt, Staatsangehörigkeit und Wohnsitzland des wirtschaftlichen Eigentümers sowie Art und Umfang des wirtschaftlichen Interesses beinhalten.
10. In der Stellungnahme 1/2017 haben wir einige die **Grundsätze der Zweckbindung und der Verhältnismäßigkeit** betreffende Bedenken gegen die durch die fünfte Geldwäscherichtlinie eingeführten Änderungen geäußert. Insbesondere wurde von uns beanstandet, dass der Richtlinienvorschlag keine ausreichenden Garantien dafür vorsah, dass verhindert wird, dass personenbezogene Daten, die für die Zwecke der Bekämpfung von Geldwäsche und Terrorismusfinanzierung erfasst wurden, zu anderen Zwecken, etwa zur Bekämpfung der **Steuerhinterziehung** oder zur Verbesserung der Transparenz von Unternehmen, verwendet werden. Ferner wurde empfohlen, ordnungsgemäß zu prüfen, **ob die vorgesehenen politischen Maßnahmen in einem angemessenen Verhältnis zu den angestrebten Zielen stehen**, insbesondere im Hinblick auf die Anwendung des risikobasierten Ansatzes, den umfassenderen Zugang der zentralen Meldestellen zu Informationen über Finanztransaktionen sowie die Ausweitung des Zugangs sowohl der zuständigen Behörden als auch der Öffentlichkeit zu Informationen über wirtschaftliche Eigentümer. Was Letzteres angeht, wurde von uns empfohlen, den Zugang auf die zuständigen Strafverfolgungsbehörden zu beschränken.

### 3. ANMERKUNGEN UND EMPFEHLUNGEN

#### 3.1. Erste Säule: Gewährleistung der wirksamen Umsetzung des bestehenden EU-Rahmens zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung

11. Der EDSB teilt die im Aktionsplan vertretene Auffassung, dass die erste Priorität der von der Kommission ergriffenen Initiativen zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung die strikte und wirksame **Umsetzung** der EU-Vorschriften zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung durch die Mitgliedstaaten sein

muss. Dazu gehört auch, dass der Datenschutzrahmen bei der Umsetzung der Maßnahmen zur Bekämpfung von Geldwäsche und Terrorismus in vollem Umfang eingehalten wird.

12. Aus der Perspektive des Datenschutzes kommt der **Einrichtung der zentralen Bankkontenmechanismen und der Register wirtschaftlicher Eigentümer** besondere Bedeutung zu, da diese darauf abzielen, Datenbanken, die eine große Menge personenbezogener Daten enthalten (z. B. Name, Geburtsdatum, Staatsangehörigkeit, Wohnsitzland, Bankverbindung usw.), zu vernetzen. Der EDSB begrüßt deshalb die von der Kommission gegebene Zusage, die Einrichtung dieser zentralen Register genauestens zu überwachen, um sicherzustellen, dass die eingespeisten Daten von hoher Qualität<sup>13</sup> und, soweit möglich, auf dem neuesten Stand sind, denn damit wird dem Grundsatz der Richtigkeit gemäß Artikel 5 Absatz 1 Buchstabe d DSGVO Rechnung getragen.
13. Die fünfte Geldwäscherichtlinie schreibt vor, dass die zentralen automatischen Mechanismen (im Folgenden: zentrale Bankkontenmechanismen) bis zum 10. September 2020 einzurichten sind.<sup>14</sup> Dabei handelt es sich um **zentrale automatische Mechanismen** wie zentrale Register oder zentrale elektronische Datenabrufsysteme, mit denen die natürlichen oder juristischen Personen, die bei Kreditinstituten Zahlungskonten, Bankkonten oder Schließfächer innehaben oder kontrollieren, ermittelt werden können.<sup>15</sup>
14. In ihrem Bericht an das Europäische Parlament und den Rat über die Vernetzung der zentralen automatischen Mechanismen der Mitgliedstaaten für Bankkonten<sup>16</sup> kam die Kommission zu dem Schluss, dass die **Vernetzung dieser Mechanismen** möglich sei. Der EDSB begrüßt es, dass die Kommission in diesem Bericht, in dem die verschiedenen IT-Lösungen auf Unionsebene, die als Modelle für die Vernetzung dieser zentralen Mechanismen dienen können, bewertet werden, den Datenschutzgrundsätzen Rechnung trägt; die Notwendigkeit, die über die Vernetzungsplattform zugänglichen Informationen auf den notwendigen Mindestumfang zu beschränken (**Datenminimierung**) sowie darauf zu achten, dass der Umfang des Zugangs zu personenbezogenen Daten in angemessenem Verhältnis zu den mit der Geldwäscherichtlinie verfolgten Zielen steht (**Grundsatz der Verhältnismäßigkeit**), wird betont.<sup>17</sup>
15. Ferner heißt es im Aktionsplan, dass die noch laufenden Arbeiten an der Vernetzung der **zentralen Register wirtschaftlicher Eigentümer** für Gesellschaften und andere juristische Personen vorangehen und die Vernetzung über die zentrale Europäische Plattform<sup>18</sup> bis zum 10. März 2021<sup>19</sup> erfolgen wird. Der EDSB erinnert daran, dass diese Register, die Verpflichteten im Rahmen von Verfahren zur Feststellung der Kundenidentität (CDD-Verfahren) zugänglich sind, personenbezogene Daten der wirtschaftlichen Eigentümer verarbeiten, und zwar mindestens Namen, Monat und Jahr der Geburt, Staatsangehörigkeit und Wohnsitzland des wirtschaftlichen Eigentümers sowie Art und Umfang seines wirtschaftlichen Interesses.<sup>20</sup> Es ist deshalb besonders wichtig, dass diese Register auf dem neuesten Stand gehalten und sämtliche angemessenen Maßnahmen getroffen werden, um sicherzustellen, dass alle unzutreffenden personenbezogenen Daten unverzüglich gelöscht oder berichtigt werden, so wie in Artikel 5 Absatz 1 Buchstabe d DSGVO vorgesehen. Dies wurde auch vom Parlament in seiner jüngsten Entschließung zum Aktionsplan (2020/2686(RSP)) hervorgehoben, in der es die Kommission aufforderte, sich mit dem Mangel an ausreichenden und korrekten Daten in den nationalen Registern wirtschaftlicher Eigentümer zu befassen, und forderte, Überprüfungsmechanismen in Bezug auf die Korrektheit der Daten vorzusehen, um sicherzustellen, dass diese ordnungsgemäß funktionieren und der Öffentlichkeit Zugang zu hochwertigen Daten gewähren.<sup>21</sup>

16. Wengleich die Arbeiten an der Vernetzung sowohl der nationalen zentralen automatischen Mechanismen als auch der zentralen Register wirtschaftlicher Eigentümer noch nicht abgeschlossen sind, begrüßt der EDSB, dass im Aktionsplan die Wichtigkeit der **Einhaltung der Datenschutzgrundsätze bei der Vernetzung dieser Mechanismen** hervorgehoben wird. Da die Vernetzung öffentlichen Behörden verschiedener Art, nämlich sowohl Strafverfolgungsbehörden als auch zentralen Meldestellen, Zugang zu zentralen Registern ermöglichen wird, ist es wichtig, bei der Vernetzung darauf zu achten, dass die Grundsätze des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen im Sinne von Artikel 25 DSGVO in die Mechanismen eingebettet und strenge Datenschutzgarantien festgelegt werden, insbesondere in Bezug auf die Zugangsrechte und die Richtigkeit der Daten. Diesbezüglich weist der EDSB auf die Stellungnahme 5/2018 zum Datenschutz durch Technikgestaltung<sup>22</sup> hin, in der im Hinblick auf die Implementierung angemessener technischer und operativer Garantien Beispiele für **Methoden zur Feststellung der Anforderungen an den Schutz der Privatsphäre und den Datenschutz und deren Einbettung in die technischen Prozesse zum Schutz der Privatsphäre** gegeben werden. Des Weiteren empfehlen wir, bei der Vernetzung die Empfehlungen in unserer Stellungnahme zu einem Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zur Änderung der Richtlinien 89/666/EWG, 2005/56/EG und 2009/101/EG in Bezug auf die Vernetzung von Zentral-, Handels- und Gesellschaftsregistern<sup>23</sup> gebührend zu berücksichtigen. Insbesondere verweisen wir auf unsere früheren Empfehlungen in Bezug auf die **Governance des Netzwerks, der Funktionen, Zuständigkeiten und Aufgaben** der Beteiligten sowie in Bezug auf die Datenschutzgarantien für **Datenübermittlungen an Drittländer**. Detaillierte Leitlinien für die solide Regelung von IT-Governance und IT-Management in Bezug auf diese vernetzten Datenbanken sind den vom EDSB herausgegebenen Leitlinien zum Schutz personenbezogener Daten für die Bereiche IT-Governance und IT-Management der EU-Institutionen zu entnehmen.<sup>24</sup>

### 3.2. Zweite Säule: Schaffung eines verbesserten Regelwerks

17. Der EDSB teilt die Auffassung, dass es die Bekämpfung der Geldwäsche erheblich erleichtern würde, wenn die AML/CFT-Vorschriften durch Annahme einer Verordnung, deren Hauptvorschriften direkt anwendbar sind und die vom Gerichtshof der Europäischen Union einheitlich ausgelegt werden, harmonisiert würden. Wir würden die weitere Harmonisierung dieser Vorschriften auf Unionsebene daher begrüßen, weil sie nicht nur der Bekämpfung von Geldwäsche und Terrorismusfinanzierung zugutekäme, sondern auch die Datenschutzgarantien in diesem Bereich auf europäischer Ebene verbessern und vereinheitlichen würde.
18. Diesbezüglich werden im Aktionsplan einige wichtige Punkte vorgeschlagen, die in einer künftigen Verordnung geregelt werden könnten, z. B. die Liste der Verpflichteten, die kundenbezogenen Sorgfaltspflichten, die internen Kontrollen, die Meldepflichten sowie die Bestimmungen über die Register wirtschaftlicher Eigentümer und die zentralen Bankkontenmechanismen. Wie bereits erwähnt, sind diese Bereiche für das Recht auf Datenschutz und Schutz der Privatsphäre von erheblicher Relevanz, weil es um die Verarbeitung einer erheblichen Menge personenbezogener Daten geht.
19. Der EDSB begrüßt die Absicht der Kommission, **bei den im verbesserten Regelwerk vorgesehenen neuen Maßnahmen einem risikobasierten Ansatz** zu folgen, der bei geringer Gefahrenlage nur geringe Grundrechtseingriffe gestattet. Ein solcher Ansatz steht mit den Datenschutzgrundsätzen sowie insbesondere mit dem Erfordernis in Einklang, die

Notwendigkeit und Verhältnismäßigkeit gesetzgeberischer Maßnahmen im Hinblick auf deren Auswirkungen auf die Rechte auf den Schutz der Privatsphäre und der personenbezogenen Daten zu bewerten. Leitlinien zu diesem Thema sind den **Leitlinien des EDSB für die Bewertung der Verhältnismäßigkeit von Maßnahmen, die die Grundrechte auf Privatsphäre und den Schutz personenbezogener Daten einschränken**<sup>25</sup>, zu entnehmen.

20. Der EDSB hat bereits in der Vergangenheit hervorgehoben, dass es wichtig ist, in den **Verfahren zur Erfüllung der kundenbezogenen Sorgfaltspflichten** (CDD-Verfahren) klare Garantien für die Einhaltung des **Rechts auf Information**<sup>26</sup> vorzusehen. Zu den dann in der vierten Geldwäscherichtlinie berücksichtigten Empfehlungen zählte die Garantie, dass der Kunde bei der Datenerfassung darüber zu informieren ist, zu welchem/n Zwecke(n) die Daten erforderlich sind und verarbeitet werden. Dies ist wichtig, da zum Beispiel für die Begründung der Geschäftsbeziehung erforderliche Daten gleichzeitig zu Geschäftszwecken (nämlich die Überprüfung der Kundenidentität) und für CDD-Zwecke (nämlich die Geldwäschebekämpfung) erfasst und verwendet werden. Diesbezüglich bestimmt Artikel 41 Absatz 3 der vierten Geldwäscherichtlinie, dass *„[d]ie Verpflichteten ... neuen Kunden die nach Artikel 10 der Richtlinie 95/46/EG vorgeschriebenen Informationen zur Verfügung [stellen], bevor sie eine Geschäftsbeziehung begründen oder gelegentliche Transaktionen ausführen. Diese Informationen umfassen insbesondere einen allgemeinen Hinweis zu den rechtlichen Pflichten der Verpflichteten gemäß der vorliegenden Richtlinie bei der Verarbeitung personenbezogener Daten zu Zwecken der Verhinderung von Geldwäsche und Terrorismusfinanzierung gemäß Artikel 1 der vorliegenden Richtlinie.“* Diese Empfehlungen haben auch nach Einführung der DSGVO noch Bestand, und wir rufen die Kommission auf, sie auch bei der Formulierung künftiger Bestimmungen zu berücksichtigen.
21. Unsere Stellungnahme von 2013 zum Vorschlag für die vierte Geldwäscherichtlinie enthielt die Empfehlung, dass der Gesetzgeber die Art der Daten klarstellen sollte, die im Rahmen der gewöhnlichen wie auch der verstärkten kundenbezogenen Sorgfaltspflichten (für die Überprüfung von politisch exponierten Personen und solchen politisch exponierten Personen bekanntermaßen nahestehenden Personen) sowie bei Risikobewertungen zu berücksichtigen sind, um willkürliche Entscheidungen und Diskriminierungen zu verhindern und die Einhaltung des **Grundsatzes der Datenminimierung** zu gewährleisten. Bei den heutigen CDD-Verfahren werden Daten verarbeitet, die die Kundenidentität, das wirtschaftliche Eigentum an juristischen Personen, den Zweck und die angestrebte Art der Geschäftsbeziehung sowie die Überprüfung der im Verlauf der Geschäftsbeziehung ausgeführten Transaktionen, einschließlich erforderlichenfalls der Herkunft der Mittel, betreffen.<sup>27</sup> Im Falle von politisch exponierten Personen, Familienangehörigen oder Personen, die politisch exponierten Personen bekanntermaßen nahestehen, erfordern die verstärkten kundenbezogenen Sorgfaltspflichten, dass der Verpflichtete die Zustimmung seiner Führungsebene einholt, bevor er Geschäftsbeziehungen zu diesen Personen aufnimmt oder fortführt, dass er angemessene Maßnahmen ergreift, um die Herkunft des Vermögens und der Gelder, die im Rahmen von Geschäftsbeziehungen oder Transaktionen mit diesen Personen eingesetzt werden, zu bestimmen, und dass er die Geschäftsbeziehung einer verstärkten fortlaufenden Überwachung unterzieht.<sup>28</sup> Verpflichtete, die im Zuge von CDD-Verfahren Kundendaten erfassen oder verarbeiten, sollten deshalb sicherstellen, dass alle personenbezogenen Daten, die sie anfordern, bezogen auf die Zwecke der kundenbezogenen Sorgfaltspflicht **dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt** sind.

22. Die CDD-Verfahren sollten auch mit der DSGVO in Einklang stehende Datenschutzgarantien enthalten, um z. B. sicherzustellen, dass über natürliche Personen, die den Regeln zur Feststellung der Kundenidentität (Know-Your-Customer) unterliegen, **keine Entscheidungen getroffen werden, die auf personenbezogenen Daten beruhen, die entweder gar nicht hätten erfasst werden dürfen** bzw. für die Begründung der Geschäftsbeziehung gar nicht notwendig waren oder die **für einen anderen, damit nicht zu vereinbarenden Zweck wiederverwendet** wurden. Die CDD-Bestimmungen sind auch auf die Grenzen abzustimmen, die gemäß Artikel 22 DSGVO für die automatisierte Entscheidung im Einzelfall und Profiling gelten, und zwar insbesondere, wenn diese CDD-Verfahren dazu führen könnten, dass hinsichtlich der Kundenaktivitäten eine Verdachtsmeldung (Suspicious Activity Report (SAR)) erstattet wird.
23. Wir merken an, dass die CDD-Verfahren im Zuge der in alle Lebensbereiche Eingang haltenden Digitalisierung für die Feststellung und Überprüfung der Kundenidentität künftig auch online (also aus der Ferne) stattfinden könnten. Für diesen Fall hebt der EDSB hervor, dass die **CDD-Digitalisierung** mit der Annahme der zur Gewährleistung der Sicherheit der **personenbezogenen Daten** notwendigen Maßnahmen einhergehen muss, insbesondere mit Maßnahmen zum Schutz vor unbefugter oder rechtswidriger Verarbeitung personenbezogener Daten und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung (Integrität und Vertraulichkeit). Bei der Digitalisierung von CDD-Verfahren sollte der **Grundsatz des Datenschutzes durch Technikgestaltung** von Anfang an in solcher Weise berücksichtigt werden, dass die Digitalisierung die Ausübung der die personenbezogenen Daten betreffenden Rechte ermöglicht. Abschließend erinnert der EDSB daran, dass seit dem Inkrafttreten der DSGVO alle Rechtspersonen sicherstellen müssen, dass sie die Einhaltung der Datenschutzpflichten nachweisen können (**Grundsatz der Rechenschaftspflicht**). In CDD-Verfahren müssen die Verpflichteten – als die für die Verarbeitung Verantwortlichen – ein Verzeichnis aller Verarbeitungstätigkeiten, die ihrer Zuständigkeit unterliegen, führen, das der Datenschutzaufsichtsbehörde auf Anfrage zur Verfügung zu stellen ist.
24. Im Aktionsplan wird dafür eingetreten, den Geltungsbereich der EU-Rechtsvorschriften zur Geldwäschebekämpfung zu erweitern, um den Auswirkungen technologischer Innovationen und Entwicklungen bei internationalen Standards Rechnung zu tragen. Der EDSB begrüßt, dass ausdrücklich erwähnt wird, dass **neue technologische Lösungen, die die Aufdeckung verdächtiger Transaktionen und Aktivitäten verbessern könnten, den Datenschutzregeln genügen müssen**, und empfiehlt, dass diese Lösungen den Grundsätzen des Datenschutzes durch Technikgestaltung (data protection by design) und datenschutzfreundliche Voreinstellungen (data protection by default) genügen sollten; insoweit wird auf die Stellungnahme 5/2018 des EDSB zum Schutz der Privatsphäre durch Technikgestaltung verwiesen.

### 3.3. Dritte Säule: Einführung einer auf EU-Ebene angesiedelten Aufsicht

25. Im Aktionsplan sieht die Kommission vor, ein **integriertes Aufsichtssystem zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung auf EU-Ebene** zu schaffen, das eine einheitliche und hohen Qualitätsansprüchen genügende Anwendung des Regelwerks für die Bekämpfung von Geldwäsche und Terrorismusfinanzierung in der gesamten EU gewährleistet und auch eine effiziente Zusammenarbeit zwischen allen einschlägigen zuständigen Behörden fördert.

26. Laut dem Aktionsplan können die Befugnisse, die der auf EU-Ebene zuständigen AML/CFT-Aufsicht in alleiniger oder in gemeinsamer Zuständigkeit mit nationalen Aufsichtsstellen übertragen werden, die Ermächtigung beinhalten, die Dokumentation über Transaktionen und Kunden zu überprüfen, um die ordnungsgemäße Umsetzung der internen Vorschriften durch die der Aufsicht unterliegenden Unternehmen sicherzustellen.<sup>29</sup> Der EDSB besteht darauf, dass es wichtig ist, dass der künftige Legislativvorschlag für die Einführung einer auf EU-Ebene angesiedelten Aufsicht zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung eine klare **Rechtsgrundlage für die Verarbeitung personenbezogener Daten** sowie klare Angaben zum Zweck und zu den Grenzen der betreffenden Verarbeitung enthält, so wie in Artikel 5 Absatz 1 der Verordnung (EU) 2018/1725 vorgesehen.
27. Die vorgesehene Aufsicht wird wahrscheinlich auch die Zusammenarbeit auf zwei Ebenen beinhalten: zum einen unter **mehreren Mitgliedstaaten** im Rahmen des grenzüberschreitenden Informationsaustauschs, zum anderen unter **verschiedenen Behörden** eines oder mehrerer Mitgliedstaaten; in der Anfangsphase unter anderem mit den zuständigen Behörden auf dem Gebiet der Aufsicht über die Kreditinstitute und die Stabilität des Finanzsystems sowie in späteren Phasen mit Ermittlungs- und Strafverfolgungsbehörden. **Der EDSB empfiehlt, dass schon das Rechtsinstrument**, durch das die auf EU-Ebene angesiedelte Aufsicht zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung geschaffen wird, **spezifische Regeln über den Informationsaustausch und die Informationsweitergabe vorsehen sollte, die die notwendigen Datenschutzgarantien berücksichtigen.**
28. Soweit die Funktionen und Befugnisse der künftigen auf EU-Ebene angesiedelten Aufsicht zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung die mögliche Zusammenarbeit der neuen Behörde mit Drittländern oder internationalen Organisationen vorsieht, sollte der Gründungsakt **spezifische Bestimmungen über die für die internationale Übermittlung operativer personenbezogener Daten geltenden Bedingungen** enthalten, mit angemessenen Garantien und für bestimmte Situationen geltende Ausnahmen.<sup>30</sup> Der EDSB erinnert daran, dass die betreffenden Bestimmungen den in den Artikeln 46 bis 51 sowie 94 der Verordnung (EU) 2018/1725 genannten Bedingungen genügen und geeigneten Datenschutzgarantien unterliegen müssen.

#### 3.4. Vierte Säule: Einrichtung eines Unterstützungs- und Kooperationsmechanismus für die zentralen Meldestellen

29. Da illegale Aktivitäten häufig mit grenzüberschreitenden Transaktionen bzw. Transaktionen zwischen verschiedenen Instituten verbunden sind, ist ein **starker und wirksamer Mechanismus zur Koordinierung der zentralen Meldestellen**, die als die „Knotenpunkte der Finanzermittlung“ („hubs of financial intelligence“)<sup>31</sup> gelten, ein wesentliches Element der Geldwäschebekämpfung. Noch gibt es allerdings nur wenig gemeinsame Analysen derartiger Aktivitäten und relevanter Faktoren durch die zentralen Meldestellen der Mitgliedstaaten und andere Behörden. In der Praxis gibt es deshalb möglicherweise gesetzliche und operative Schlupflöcher, die sich Straftäter zur Begehung von Straftaten im Bereich der Geldwäsche oder Terrorismusfinanzierung zunutze machen können.
30. Die grenzüberschreitende Koordinierung erfordert den Einsatz **maßgeschneiderter und wirksamer Instrumente und Verfahren**, die den Informationsaustausch und Datenabgleich ermöglichen, dabei jedoch in vollem Umfang den Datenschutzanforderungen genügen. Diesbezüglich ist der Datenschutz als für den komplexen Analyseprozess zur Verhinderung

und Aufdeckung von Geldwäsche und anderen Straftaten unverzichtbar anzusehen – keinesfalls als ein entgegenstehendes Hindernis.

### **FIU.net**

31. Seit fast 20 Jahren wird die Zusammenarbeit unter den zentralen Meldestellen in der Europäischen Union durch ein Netzwerk für den Informationsaustausch (das sogenannte **FIU.net**) ermöglicht<sup>32</sup>. In ihrer „*Mitteilung über Wege zu einer besseren Umsetzung des Rechtsrahmens der EU für die Bekämpfung von Geldwäsche und Terrorismusfinanzierung*“ hat die Kommission anerkannt, dass es auch heute noch wiederholte technische Probleme des FIU.net gibt, die den zentralen Meldestellen den Informationsaustausch erschweren, was einen geringeren Informationsaustausch und Datenabgleich unter den zentralen Meldestellen zur Folge hatte.<sup>33</sup> Im Bericht wird erklärt, dass fehlende Rechtsvorschriften in Bezug auf den Informationsaustausch zwischen den zentralen Meldestellen der Mitgliedstaaten und den zentralen Meldestellen von Drittländern zu einem nicht harmonisierten Ansatz für diesen Informationsaustausch führten. Diese rechtlichen und praktischen Hindernisse wirken sich unweigerlich auf die Richtigkeit und Aktualität der Informationen von FIU.net aus und stellen deshalb ein Risiko für die Rechte auf den Schutz der Privatsphäre und der personenbezogenen Daten dar.
32. Um diesen Problemen entgegenzuwirken, ist es laut dem Aktionsplan dringend notwendig, in die Entwicklung von FIU.net zu investieren sowie eine geeignete Lösung für seine Verwaltung zu finden.
33. Was die Zukunft von FIU.net betrifft<sup>34</sup>, hat die Kommission die künftige auf EU-Ebene angesiedelte Aufsicht über die Bekämpfung von Geldwäsche und Terrorismusfinanzierung als eine Stelle benannt, die das **Hosting des Netzwerks** übernehmen könnte, aber auch andere Lösungsmöglichkeiten aufgezeigt, z. B. die **Stärkung des Mandats von Europol**, um eine Rechtsgrundlage für das Hosting des Netzwerks durch Europol zu schaffen.<sup>35</sup> Für den Fall, dass bis Ende 2020 keine Lösung gefunden werden sollte, hat die Kommission die Absicht geäußert, vorläufig die Verwaltung von FIU.net zu übernehmen, um das kontinuierliche und unterbrechungsfreie Funktionieren des Systems zu gewährleisten.
34. Welche Rolle die Kommission, soweit sie das Hosting von FIU.net übernimmt, in datenschutzrechtlicher Hinsicht spielen wird (d. h. ob sie Verantwortlicher, gemeinsam Verantwortlicher oder Auftragsverarbeiter handelt), muss noch bestimmt werden; der EDSB erinnert jedoch daran, dass die Verarbeitung personenbezogener Daten über das Netzwerk auf einer gültigen Rechtsgrundlage beruhen muss. Diesbezüglich merken wir an, dass gemäß Artikel 51 der vierten Geldwäscherichtlinie „*[d]ie Kommission ... die erforderliche Unterstützung leisten [kann], um die Koordinierung, einschließlich des Informationsaustauschs zwischen den zentralen Meldestellen innerhalb der Union, zu erleichtern*“. Ohne dass hier einer eingehenderen Prüfung vorgegriffen werden soll, kann man wohl sagen, dass diese Bestimmung, auch wenn sie nicht ausdrücklich auf die Verarbeitung personenbezogener Daten Bezug nimmt, eine gewisse Rechtsgrundlage für die Verwaltung von **FIU.net** bieten dürfte, da die Verarbeitung personenbezogener Daten normalerweise als eine Verarbeitung anzusehen wäre, die für die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung der Kommission übertragener öffentlicher Gewalt erfolgt, erforderlich ist (siehe Artikel 6 DSGVO und Artikel 5 der Verordnung (EU) 2018/1725).

### **Der Unterstützungs- und Kooperationsmechanismus für die zentralen Meldestellen**

35. Was den Unterstützungs- und Kooperationsmechanismus für die zentralen Meldestellen allgemein angeht, **merkt der EDSB an, dass die zentralen Meldestellen in den verschiedenen Mitgliedstaaten unterschiedlichen institutionellen Modellen folgen und deshalb mit verschiedenen Befugnissen ausgestattet sind.** So gibt es zum einen zentrale Meldestellen, die **Verwaltungsbehörden** sind, die Verdachtsmeldungen prüfen und zur Ermittlung an Strafverfolgungsbehörden weiterreichen, wenn es Anzeichen dafür gibt, dass eine gemeldete Transaktion möglicherweise einen Straftatbestand erfüllt. Zum anderen gibt es zentrale Meldestellen, die mit Ermittlungsbefugnissen im Bereich der Bekämpfung von Geldwäsche und Terrorismusfinanzierung ausgestattete **Strafverfolgungsbehörden** sind. Außerdem gibt hybride Formen beider Modelle, die unterschiedliche Befugnisse vorsehen. Wie die Kommission in ihrem Bericht über die Bewertung des Rahmens für die Zusammenarbeit zwischen den zentralen Meldestellen für Geldwäsche-Verdachtsanzeigen (FIU)<sup>36</sup> festgestellt hat, haben die Unterschiede in Status, Befugnissen und Organisation der zentralen Meldestellen weiterhin **Auswirkungen darauf, wie die FIU an die entsprechenden Daten gelangen und wie sie sie miteinander austauschen.** Unter dem Gesichtspunkt des Datenschutzes besteht wegen solcher Verzerrungen, die sich aus dem unterschiedlichen Charakter der zentralen Meldestellen ergeben, ein ernstzunehmendes Risiko, dass bei Informationsverwaltung und -austausch der Grundsatz der Zweckbindung nicht eingehalten wird.
36. Ferner erinnert der EDSB daran, dass gemäß Erwägungsgrund 56 der vierten Geldwäscherichtlinie ein Austausch von Informationen über Geldwäsche und Terrorismusfinanzierung zwischen den zentralen Meldestellen – **zu Analysezwecken, ohne dass diese Informationen weiterverarbeitet oder weitergegeben werden** – erlaubt sein sollte, sofern der Informationsaustausch den Grundprinzipien des nationalen Rechts nicht zuwiderläuft. Der EDSB empfiehlt deshalb, die **Voraussetzungen für den Zugang der zentralen Meldestellen zu Informationen über Finanztransaktionen sowie für ihren Informationsaustausch** bereits in dem von der Kommission vorgesehenen Legislativvorschlag, durch den ein Unterstützungs- und Kooperationsmechanismus für die zentralen Meldestellen der Mitgliedstaaten eingerichtet werden soll, ausdrücklich und klar zu regeln. Des Weiteren halten wir, was die Grundsätze der Verhältnismäßigkeit und Zweckbindung angeht, an unserer bereits in der Stellungnahme 1/2017 vertretenen Ansicht zu einer rechtlichen Konfiguration fest, bei der sich die Befugnisse der zentralen Meldestellen nicht mehr auf „Untersuchungen“, sondern auf „Erkenntnisse“ stützen und die zentralen Meldestellen für ihre eigenen Analysen und Erkenntnisse Informationen bei Verpflichteten anfordern können, auch ohne dass ihnen zuvor verdächtige Transaktionen gemeldet wurden.<sup>37</sup> Wie von uns bereits in der genannten Stellungnahme ausgeführt wurde, käme letztere Vorgehensweise eher einem Data-Mining als einer gezielten Untersuchung gleich, was natürlich Auswirkungen auf die personenbezogene Daten betreffenden Rechte hätte.

### **3.5. Fünfte Säule: Durchsetzung strafrechtlicher Bestimmungen und Informationsaustausch auf Unionsebene**

37. In Bezug auf den im Aktionsplan enthaltenen Aufruf zur verbesserten Koordinierung zwischen den Strafverfolgungsbehörden und den zentralen Meldestellen der Mitgliedstaaten im Bereich der Finanzausmittlung und unter Berücksichtigung der Unterschiede bei Art und Umfang der Befugnisse (Verwaltungstätigkeit bzw. Strafverfolgung) möchte der EDSB hervorheben, dass **Koordination und Datenaustausch stets dem Datenschutzrahmen genügen müssen.** Auch die technischen Mittel, die für den Informationsaustausch zwischen den Behörden eingesetzt werden, müssen angemessene technische und organisatorische

Vorkehrungen (einschließlich Verschlüsselung und Anonymisierung) vorsehen, um die Daten vor unbeabsichtigter oder unrechtmäßiger Zerstörung, unbeabsichtigtem Verlust, Veränderung oder unrechtmäßiger Schädigung zu schützen.

38. Im Aktionsplan spricht sich die Kommission dafür aus, im Bereich der Finanzausmittlung auf öffentlich-private Partnerschaften (ÖPP) zu setzen, und zwar im Wesentlichen in zwei Formen: 1) in der Form des Informationsaustauschs zu **Typologien und Trends** zwischen zentralen Meldestellen und Strafverfolgungsbehörden auf der einen Seite und Verpflichteten auf der anderen Seite sowie 2) in der Form der Weitergabe von **operativen Informationen über Verdächtige** durch Strafverfolgungsbehörden an Verpflichtete zum Zwecke der Überwachung der Transaktionen der betreffenden Verdächtigen. Diese Initiative steht mit der seit einigen Jahren von der Financial Action Task Force (**FATF**) vertretenen Auffassung in Einklang, dass zum Schutz der Integrität des internationalen Finanzsystems den ÖPP eine aktivere Rolle in Bezug auf Finanzausmittlungen zukommen sollte.<sup>38</sup>
39. Was die **erste Art von ÖPP** angeht, wird die **Idee der Zusammenarbeit von Strafverfolgungsbehörden, zentralen Meldestellen und Privatsektor** im Bereich der Gestaltung der politischen Debatte, in Diskussionsforen wie auch bei der Erforschung und Analyse von Typologien und Trends zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung **vom EDSB begrüßt und unterstützt**. Wir erinnern daran, dass in ähnlichen Bereichen, etwa in der Cybersicherheit, beim Hochleistungsrechnen (HPC), in der Robotik oder bei künftigen Internettechnologien<sup>39</sup> erfolgreich von ÖPP Gebrauch gemacht worden ist, wobei die Datenschutzerfordernisse den Informationsaustausch geprägt haben und in die Forschungsprozesse integriert waren, ohne dass dies in besonderem Maße Anlass zu Bedenken bezüglich ihrer Implementierung gegeben hätte.
40. Der EDSB begrüßt die Entschließung des Parlaments zum Aktionsplan<sup>40</sup>, in der es ÖPP in Form einer Dreierplattform ausdrücklich befürwortet und hervorhebt, dass diese Art von ÖPP verpflichtet sind, in ihrer Arbeit die Grenzen der geltenden Datenschutzvorschriften und die Grundrechte strikt einzuhalten. Der EDSB schließt sich der Forderung des Parlaments an, dass die Kommission **einen klaren Rechtsrahmen für diese Plattformen vorschlagen** soll, weil so auch die Einhaltung der für den Informationsaustausch und Datenschutz geltenden Regeln sichergestellt wird.
41. Was ÖPP angeht, im Rahmen derer die Weitergabe **operativer Informationen über einschlägige Verdächtige von Strafverfolgungsbehörden an Verpflichtete** vorgesehen ist, hat der EDSB, ohne eine Beurteilung der zugrunde liegenden politischen Erwägungen vornehmen zu wollen, **Bedenken, dass eine solche Vorgehensweise zu einem hohen Risiko für die Rechte natürlicher Personen auf Privatsphäre und Datenschutz führen würde**.
42. Der EDSB erinnert an unsere Stellungnahme 1/2017, in der hervorgehoben wurde, dass bei der Geldwäschebekämpfung die Untersuchung und Strafverfolgung krimineller Tätigkeiten den zuständigen Behörden vorbehalten sind. Unter keinen Umständen darf einer Privatperson förmlich oder informell, direkt oder indirekt eine Aufgabe in der Strafverfolgung übertragen werden.<sup>41</sup> Würden ÖPP geschaffen, im Rahmen derer es privaten Einrichtungen (d. h. den Verpflichteten) gestattet sein sollte, Personen (bei denen es sich um ihre Kunden handelt) auf der Grundlage aktueller operativer Informationen, hinsichtlich derer die Strafverfolgungsbehörden noch ermitteln, zu überwachen, so würde dadurch ein Präzedenzfall geschaffen, der unserer Ansicht nach, was den Datenschutz angeht, sehr riskant wäre.
43. Nach dem Rahmen für die Geldwäschebekämpfung ist die Rolle der Verpflichteten darauf beschränkt, den zentralen Meldestellen durch sogenannte Verdachtsmeldungen verdächtige

Aktivitäten zu melden. Dabei fließen die Informationen nur in die eine Richtung; die Verpflichteten erhalten von den zentralen Meldestellen oder Strafverfolgungsbehörden keinerlei Rückmeldung darüber, was die Prüfung ergeben hat oder wie mit den gemeldeten Informationen verfahren wurde. Unter dem Gesichtspunkt des Datenschutzes stellt dies eine Garantie für den Schutz der Privatsphäre der natürlichen Personen dar, da die Verpflichteten in keiner Weise an der Verarbeitung der Informationen über die möglicherweise strafbaren Transaktionen, die als verdächtig gemeldet wurden, beteiligt sind; dies sind sensible Informationen, die wegen ihrer Auswirkungen auf die Grundrechte der betroffenen Personen ausschließlich staatlichen Behörden zugänglich sein sollten.

44. Unbeschadet eines etwaigen späteren Vorbringens ist der EDSB der Ansicht, dass es zurzeit keine zwingenden Gründe gibt, die es rechtfertigen würden, Privatpersonen Zugang zu sensiblen personenbezogenen Daten natürlicher Personen, die kriminelle Aktivitäten oder laufende Ermittlungen wegen Straftatverdachts betreffen, zu geben; solche Daten sind zurzeit allein den zuständigen staatlichen Behörden vorbehalten, und dabei sollte es auch bleiben. Ferner erinnert der EDSB daran, dass eine Maßnahme dem in Artikel 52 Absatz 1 der Charta niedergelegten Grundsatz der Verhältnismäßigkeit nur dann Genüge tut, wenn die Nachteile, die die Maßnahme im Hinblick auf die Grundrechtsausübung mit sich bringt, nicht schwerer wiegen als der sich aus der Maßnahme ergebende Nutzen. Insoweit sind wir der Auffassung, dass eine Maßnahme, die Privatpersonen Befugnisse zur Überwachung Verdächtiger einräumt, nur sehr schwer die Anforderungen an die Verhältnismäßigkeit und Erforderlichkeit erfüllen dürfte, und dass zunächst andere Optionen zu prüfen sind, mit denen dasselbe Ziel auf eine Weise erreicht werden kann, die weniger stark in die Grundrechte eingreift.<sup>42</sup>
45. Zweitens lässt der Austausch sensibler Daten von „Verdächtigen“ mit dem privaten Sektor Interessenkonflikte befürchten, da es sich bei den Verdächtigen möglicherweise um eigene Kunden handelt. Der EDSB hat insbesondere im Hinblick darauf Bedenken, dass den ÖPP, die für den **Austausch operativer Informationen über einschlägige Verdächtige** eingegangen werden, möglicherweise die nötige Unabhängigkeit und Autonomie fehlt; schließlich wären die Verpflichteten gehalten, ihre eigenen Kunden zu überwachen, denen sie jedoch im Rahmen ihrer Geschäftsbeziehung zur Vertraulichkeit verpflichtet sind.
46. Drittens befürchtet der EDSB bei dieser Art von ÖPP Probleme in Bezug auf den **Grundsatz der Zweckbindung**, nach dem personenbezogene Daten nur für genau festgelegte, ausdrückliche und rechtmäßige Zwecke erhoben werden und nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden dürfen. So könnten insbesondere die an ÖPP beteiligten Verpflichteten versucht sein, die Informationen, die von den Strafverfolgungsbehörden über die Plattform weitergegeben werden, **in ihre allgemeinen Datenbanken aufzunehmen, um sie später, als Teil ihrer Kundenprofile, weiterzuverwenden**.<sup>43</sup> Dadurch könnten bestimmte Kunden diskriminiert werden (z. B. diejenigen, die für die der Bank nur wenig profitabel sind, aber ein erhebliches Risiko darstellen), was wiederum die finanzielle Exklusion vulnerabler Personen und Gemeinschaften zur Folge haben könnte (im Zuge des sogenannten De-Risking, wenn Finanzunternehmen ihre Geschäftsbeziehungen zu Risikokunden kündigen oder einschränken).<sup>44</sup>
47. In der Tat ist in den wenigen Ländern der Welt, die sich für das Modell der Mitwirkung von ÖPP an Aufgaben im Bereich der Finanzermittlung<sup>45</sup> entschieden haben, zu sehen, dass derartige ÖPP Probleme aufwerfen und Anlass zu Bedenken geben; in der EU gibt es dafür nur ein einziges Beispiel, das einen ehemaligen Mitgliedstaat betrifft.<sup>46</sup> Hinzu kommt, dass sich die wenigen ÖPP, die es gibt, auf Partnerschaften für den Informationsaustausch auf

nationaler Ebene beschränken, ohne jeglichen grenzüberschreitenden Austausch von Finanzinformationen und mit einer sehr kleinen Anzahl von Beteiligten.

### **3.6. Sechste Säule: Stärkung der internationalen Dimension des EU-Rahmens**

48. Der EDSB begrüßt, dass die Kommission bestrebt ist, bei der Arbeit der FATF wie auch bei der Festlegung internationaler Standards für die Bekämpfung von Geldwäsche und Terrorismusfinanzierung eine stärkere Rolle zu spielen. In diesem Zusammenhang fordern wir die Kommission auf, sich zur Garantie der Grundrechte natürlicher Personen dafür einzusetzen, die Datenschutzgrundsätze der Union in den Compliance-Prozessen für die Bekämpfung von Geldwäsche und Terrorismusfinanzierung zu verankern. Seit der Annahme der DSGVO hat die EU gezeigt, dass sie auf die Rechtsordnungen von Drittländern Einfluss nehmen und auf die Verbesserung von deren Datenschutznormen hinwirken kann. Wir denken, dass sie dies auch weiterhin tun sollte, z. B. in Diskussionen über internationale AML/CFT-Standards für CDD-Verfahren, über das Führen von Verzeichnissen oder Verdachtsmeldungen – überall dort, wo den Rechten der natürlichen Personen, deren Daten verarbeitet werden, sowie den Grundsätzen der Datenminimierung und der Richtigkeit große Bedeutung zukommt.
49. Der EDSB begrüßt die neue Methode zur Bewertung von Drittländern mit hohem Risiko (SWD (2020) 99)<sup>47</sup>, die gleichzeitig mit dem Aktionsplan veröffentlicht wurde. Die Methode basiert auf den in Artikel 9 der vierten Geldwäscherichtlinie aufgeführten Kriterien, und die Bewertung von Drittländern mit hohem Risiko sollte mit den Ausführungen in dieser Stellungnahme in Einklang stehen.

## **4. SCHLUSSFOLGERUNGEN**

Vor diesem Hintergrund spricht der EDSB folgende Empfehlungen aus:

- Er fordert die Kommission auf, beim Erlass der einschlägigen Rechtsvorschriften auf ein angemessenes Gleichgewicht zwischen den Maßnahmen, die zur wirksamen Erreichung der im Allgemeininteresse liegenden Ziele im Bereich der Bekämpfung von Geldwäsche und Terrorismusfinanzierung (im Folgenden: AML/CFT) erforderlich sind, und dem Eingriff in die Grundrechte auf den Schutz der Privatsphäre und der personenbezogenen Daten zu achten.
- Er empfiehlt der Kommission, im Zuge der Überwachung der Umsetzung des bestehenden Rahmens für die Bekämpfung von Geldwäsche und Terrorismusfinanzierung die Einhaltung der DSGVO und des Datenschutzrahmens sicherzustellen.
- Er empfiehlt hinsichtlich der Arbeiten an der Vernetzung der zentralen Bankkontenmechanismen und der Register wirtschaftlicher Eigentümer, dass diese vor allem den Grundsätzen der Datenminimierung, der Richtigkeit sowie des Datenschutzes durch Technikgestaltung und datenschutzfreundliche Voreinstellungen Rechnung tragen sollten.
- Er schlägt vor, dass die Kommission bezüglich der im verbesserten Regelwerk vorgesehenen neuen Maßnahmen zur Bekämpfung von Geldwäsche und Terrorismus an einem risikobasierten Ansatz festhalten sollte, der bei geringer Gefahrenlage nur geringe Grundrechtseingriffe gestattet, da dies auch mit den Datenschutzgrundsätzen in Einklang steht.

- Er empfiehlt im Hinblick auf die kundenbezogenen Sorgfaltspflichten, im vorgeschlagenen Rechtsakt das Recht der Kunden, zum Zeitpunkt der Datenerfassung über den/die Zweck(e), für die die Daten erforderlich sind und verarbeitet werden, informiert zu werden, zu garantieren sowie die Einhaltung der Grundsätze der Datenminimierung, der Zweckbindung und des Datenschutzes durch Technikgestaltung sowie der Grenzen der automatisierten Entscheidung im Einzelfall sicherzustellen.
- Er empfiehlt der Kommission, in ihrem Vorschlag für die Einführung einer auf EU-Ebene angesiedelten Aufsicht über die Bekämpfung von Geldwäsche und Terrorismusfinanzierung eine Rechtsgrundlage für die Verarbeitung personenbezogener Daten sowie die nach der DSGVO und der Verordnung (EU) 2018/1725 erforderlichen Datenschutzgarantien vorzusehen, insbesondere in Bezug auf Informationsaustausch und internationale Datenübermittlungen.
- Er empfiehlt der Kommission, im Vorschlag zur Einrichtung eines Koordinierungs- und Unterstützungsmechanismus für zentrale Meldestellen die Voraussetzungen klarzustellen, unter denen zentralen Meldestellen der Zugang zu und der Austausch von Informationen über Finanztransaktionen gestattet ist.
- Er unterstützt den Aufbau öffentlich-privater Partnerschaften (ÖPP) zur Erforschung und Analyse von Typologien und Trends für die Zwecke der Bekämpfung von Geldwäsche und Terrorismusfinanzierung, wobei die sich aus der DSGVO ergebenden Grenzen einzuhalten sind.
- Er regt an, dass sich die Kommission bei der Financial Action Task Force dafür einsetzt, die Datenschutzgrundsätze in die internationalen Standards aufzunehmen.

Brüssel, den 23. Juli 2020

Wojciech WIEWIÓROWSKI  
(elektronisch gezeichnet)

---

## ANMERKUNGEN

<sup>1</sup> 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, S. 1.

<sup>2</sup> Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG, ABl. L 295 vom 21.11.2018.

<sup>3</sup> <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12176-Action-Plan-on-anti-money-laundering/public-consultation>

<sup>4</sup> Urteil vom 8. April 2014, Digital Rights Ireland und Seitlinger u. a. (C-293/12, ECLI:EU:C:2014:238).

<sup>5</sup> [https://edps.europa.eu/sites/edp/files/publication/17-06-01\\_necessity\\_toolkit\\_final\\_de.pdf](https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_de.pdf)

<sup>6</sup> [https://edps.europa.eu/sites/edp/files/publication/19-12-19\\_edps\\_proportionality\\_guidelines2\\_de.pdf](https://edps.europa.eu/sites/edp/files/publication/19-12-19_edps_proportionality_guidelines2_de.pdf)

<sup>7</sup> Richtlinie (EU) 2018/1673 des Europäischen Parlaments und des Rates vom 23. Oktober 2018

über die strafrechtliche Bekämpfung der Geldwäsche.

<sup>8</sup> Die Mitgliedstaaten müssen die sechste Geldwäscherichtlinie bis zum 3. Dezember 2020 in nationales Recht umsetzen; danach haben die Unternehmen in den Mitgliedstaaten bis zum 3. Juni 2021 Zeit, die einschlägigen Bestimmungen umzusetzen.

<sup>9</sup> In den Erwägungsgründen 22 und 33 der vierten Geldwäscherichtlinie heißt es: „Das Risiko der Geldwäsche und Terrorismusfinanzierung ist nicht in allen Fällen gleich hoch. Aus diesem Grund sollte nach einem ganzheitlichen, risikobasierten Ansatz verfahren werden. Dieser stellt nicht die Möglichkeit einer ungebührlich ausufernden Freistellung für Mitgliedstaaten und Verpflichtete dar. Er setzt eine faktengestützte Entscheidungsfindung voraus, die es ermöglicht, gezielter auf die für die Union und die dort tätigen natürlichen und juristischen Personen bestehenden Risiken der Geldwäsche und Terrorismusfinanzierung einzugehen. Das Bedürfnis der Mitgliedstaaten und der Union, die für sie bestehenden Risiken von Geldwäsche und Terrorismusfinanzierung zu ermitteln, zu verstehen und zu mindern, bildet die Grundlage des risikobasierten Ansatzes ...“

<sup>10</sup> Siehe Erwägungsgrund 19 der sechsten Geldwäscherichtlinie.

<sup>11</sup> [https://edps.europa.eu/sites/edp/files/publication/13-07-04\\_money\\_laundering\\_de.pdf](https://edps.europa.eu/sites/edp/files/publication/13-07-04_money_laundering_de.pdf)

<sup>12</sup> [https://edps.europa.eu/sites/edp/files/publication/17-02-02\\_opinion\\_aml\\_de.pdf](https://edps.europa.eu/sites/edp/files/publication/17-02-02_opinion_aml_de.pdf)

<sup>13</sup> Siehe Aktionsplan, Seite 4.

<sup>14</sup> Siehe Erwägungsgrund 53 der fünften Geldwäscherichtlinie.

<sup>15</sup> Siehe Artikel 1 Absatz 19 der fünften Geldwäscherichtlinie, durch die die Artikel 32a und 32b in die vierte Geldwäscherichtlinie eingefügt werden.

<sup>16</sup> Abrufbar unter <https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52019DC0372&qid=1598972319931&from=DE>

<sup>17</sup> Siehe Seite 6 des Berichts.

<sup>18</sup> Artikel 30 Absatz 10 der vierten Geldwäscherichtlinie in der durch die fünfte Geldwäscherichtlinie geänderten Fassung.

<sup>19</sup> Erwägungsgrund 53 der fünften Geldwäscherichtlinie.

<sup>20</sup> Artikel 30 Absatz 5 der vierten Geldwäscherichtlinie.

<sup>21</sup> Entschließung des Europäischen Parlaments vom 10. Juli 2020 zu einer umfassenden Politik der Union zur Verhinderung von Geldwäsche und Terrorismusfinanzierung – der Aktionsplan der Kommission und andere aktuelle Entwicklungen (2020/2686(RSP)), abrufbar unter [https://www.europarl.europa.eu/doceo/document/TA-9-2020-0204\\_DE.html](https://www.europarl.europa.eu/doceo/document/TA-9-2020-0204_DE.html).

<sup>22</sup> Siehe [https://edps.europa.eu/sites/edp/files/publication/18-05-31\\_preliminary\\_opinion\\_on\\_privacy\\_by\\_design\\_en\\_0.pdf](https://edps.europa.eu/sites/edp/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf)

---

<sup>23</sup> [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.C\\_.2011.220.01.0001.01.ENG&toc=OJ.C:2011:220:TOC](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.C_.2011.220.01.0001.01.ENG&toc=OJ.C:2011:220:TOC)

<sup>24</sup> [https://edps.europa.eu/sites/edp/files/publication/it\\_governance\\_management\\_de.pdf](https://edps.europa.eu/sites/edp/files/publication/it_governance_management_de.pdf)

<sup>25</sup> Siehe Endnote 6.

<sup>26</sup> Siehe Stellungnahme von 2013 des EDSB zum Vorschlag für die vierte Geldwäscherichtlinie, Nr. 13.

<sup>27</sup> Siehe Artikel 13 der vierten Geldwäscherichtlinie.

<sup>28</sup> Siehe Artikel 20-23 der vierten Geldwäscherichtlinie.

<sup>29</sup> Siehe Seite 8 des Aktionsplans.

<sup>30</sup> Siehe Artikel 94 der Verordnung (EU) 2018/1725.

<sup>31</sup> Siehe dazu den Bericht des Europäischen Parlaments „Anti-money laundering – reinforcing the supervisory and regulatory framework“ [Geldwäschebekämpfung – Stärkung des Aufsichts- und regulatorischen Rahmens].

<sup>32</sup> FIU.net ist ein dezentrales und hochentwickeltes Computernetzwerk, das die zentralen Meldestellen (Financial Intelligence Units (FIUs)) in der Europäischen Union in ihrem Kampf gegen Geldwäsche und Terrorismusfinanzierung unterstützt. Das 2002 (aufgrund des Beschlusses 2000/642/JI des Rates vom 17. Oktober 2000) in Betrieb genommene Netzwerk wurde auch in der Richtlinie 2005/60/EG (dritte Geldwäscherichtlinie) und in der derzeit geltenden vierten Geldwäscherichtlinie als Instrument für den Informationsaustausch unter zentralen Meldestellen genannt. Seit Januar 2016 ist FIU.net in Europol eingegliedert.

<sup>33</sup> Siehe die Mitteilung der Kommission an das Europäische Parlament und den Rat über Wege zu einer besseren Umsetzung des Rechtsrahmens der EU für die Bekämpfung von Geldwäsche und Terrorismusfinanzierung. COM(2019) 360 final.

<sup>34</sup> Im Dezember 2019 stellte der EDSB fest, dass die Einbettung von FIU.Net in die Systeme von Europol (SIENA) gegen die Bestimmungen über die Verarbeitung personenbezogener Daten verstieß, weil Europol nach der Europol-Verordnung nur die personenbezogenen Daten bestimmter Kategorien von Personen verarbeiten darf. Diese Bestimmungen wären nur eingehalten, wenn alle natürlichen Personen, die an verdächtigen Transaktionen beteiligt sind, als Verdächtige anzusehen wären, was aber im Hinblick auf die über FIU.net ausgetauschten Informationen und personenbezogenen Daten nicht stets der Fall sein wird. In unserer Stellungnahme gelangten wir deshalb zu dem Ergebnis, dass die technische Verwaltung von FIU.net durch Europol gegen die Europol-Verordnung verstieß. Wegen der Bedeutung von FIU.net für die Bekämpfung von Geldwäsche und Terrorismusfinanzierung auf Unionsebene haben wir jedoch die Untersagung der Verwaltung durch Europol bis zum 19. Dezember 2020 ausgesetzt, um einen reibungslosen Übergang der technischen Verwaltung von FIU.net an eine andere Stelle zu ermöglichen.

<sup>35</sup> Siehe Nr. 33 des angepassten Arbeitsprogramms der Europäischen Kommission, abrufbar unter [https://ec.europa.eu/info/sites/info/files/cwp-2020-adjusted-annexes\\_en.pdf](https://ec.europa.eu/info/sites/info/files/cwp-2020-adjusted-annexes_en.pdf)

<sup>36</sup> <https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52019DC0371&from=DE>

<sup>37</sup> Siehe Stellungnahme 1/2017 des EDSB, Nr. 52.

<sup>38</sup> Siehe <https://www.fatf-gafi.org/publications/fatfgeneral/documents/public-private-sector-partnership.html>

<sup>39</sup> <https://ec.europa.eu/digital-single-market/en/public-private-partnerships>

<sup>40</sup> Siehe Endnote 19.

<sup>41</sup> Siehe Stellungnahme 2017, Nr. 16.

<sup>42</sup> Siehe dazu das Toolkit des EDSB zu Erforderlichkeit, abrufbar unter [https://edps.europa.eu/sites/edp/files/publication/17-06-01\\_necessity\\_toolkit\\_final\\_de.pdf](https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_de.pdf)

<sup>43</sup> Tsingou, E., „Global financial governance and the developing anti-money laundering regime: What lessons for International Political Economy?“, Int Polit 47, S. 617-637 (2010). <https://doi.org/10.1057/ip.2010.32>

<sup>44</sup> Siehe <https://www.fatf-gafi.org/publications/fatfgeneral/documents/public-private-sector-partnership.html>

<sup>45</sup> [https://rusi.org/sites/default/files/201710\\_rusi\\_the\\_role\\_of\\_fisps\\_in\\_the\\_disruption\\_of\\_crime\\_maxwell\\_aringstall\\_web\\_4.2.pdf](https://rusi.org/sites/default/files/201710_rusi_the_role_of_fisps_in_the_disruption_of_crime_maxwell_aringstall_web_4.2.pdf)

<sup>46</sup> In der Europäischen Union beschränkte sich die Erfahrung mit ÖPP für Finanzermittlungen auf die Joint Money Laundering Intelligence Taskforce (JMLIT) im Vereinigten Königreich. Die JMLIT umfasste drei Untergliederungen: 1) eine operative Gruppe, die dazu diente, operative Informationen über Aktivitäten zwischen dem Finanzsektor, den Strafverfolgungsbehörden und der Finanzaufsichtsbehörde auszutauschen; 2) verschiedene Sachverständigengruppen, die dafür zuständig waren, neue und entstehende Gefahren im Bereich der Geldwäsche

---

und Terrorismusfinanzierung zu erkennen und zu bewerten und diesbezügliche Wissensprodukte wie Typologien und Warnindikatoren zu liefern; sowie 3) einen Warnservice für die allgemeine Verbreitung von Bewertungen und Typologien, der von UK Finance angeboten wird.

<sup>47</sup> [https://ec.europa.eu/info/sites/info/files/business\\_economy\\_euro/banking\\_and\\_finance/documents/200507-anti-money-laundering-terrorism-financing-action-plan-methodology\\_en.pdf](https://ec.europa.eu/info/sites/info/files/business_economy_euro/banking_and_finance/documents/200507-anti-money-laundering-terrorism-financing-action-plan-methodology_en.pdf)