



EUROPÄISCHE
KOMMISSION

Brüssel, den 8.12.2021
SWD(2021) 379 final

ARBEITSUNTERLAGE DER KOMMISSIONSDIENSTSTELLEN
BERICHT ÜBER DIE FOLGENABSCHÄTZUNG (ZUSAMMENFASSUNG)

Begleitunterlage zum

**VORSCHLAG FÜR EINE VERORDNUNG DES EUROPÄISCHEN PARLAMENTS
UND DES RATES**

**über den automatisierten Datenaustausch für die polizeiliche Zusammenarbeit
(„Prüm II“) und zur Änderung der Beschlüsse 2008/615/JI und 2008/616/JI des Rates
sowie der Verordnungen (EU) 2018/1726, (EU) 2019/817 und (EU) 2019/818 des
Europäischen Parlaments und des Rates**

{COM(2021) 784 final} - {SEC(2021) 421 final} - {SWD(2021) 378 final}

Zusammenfassung

Folgenabschätzung zum Vorschlag zur Stärkung des automatisierten Datenaustauschs auf der Grundlage des Prüm-Rahmens (Überarbeitung der Beschlüsse 2008/615/JI und 2008/616/JI des Rates)

A. Handlungsbedarf

Warum? Um welche Problematik geht es?

Die Kriminalität in ganz Europa untergräbt die Sicherheit und das Wohlergehen der EU-Bürgerinnen und -Bürger. Für eine wirksame Bekämpfung der Kriminalität benötigen die Strafverfolgungsbehörden robuste und leistungsfähige Instrumente. Wie in der EU-Strategie für eine Sicherheitsunion 2020 erwähnt, sind Zusammenarbeit und Informationsaustausch die wirksamsten Mittel zur Bekämpfung der Kriminalität und zur Durchsetzung von Recht und Gesetz.¹ Laut der Bewertung der Bedrohungslage im Bereich der schweren und organisierten Kriminalität in der EU von 2021 sind mehr als **70 % der organisierten kriminellen Gruppen in mehr als drei Mitgliedstaaten aktiv**. Selbst ein scheinbar rein lokales Verbrechen kann einen Bezug zu anderen Orten in Europa haben, an denen derselbe Täter seine Straftaten verübt hat. In diesem Zusammenhang **müssen die Strafverfolgungsbehörden in der Lage sein, Daten zeitnah auszutauschen**. In einem Raum ohne Binnengrenzen **gibt es jedoch immer noch Grenzen und Hindernisse für den Datenaustausch zwischen den Strafverfolgungsbehörden**, was zu blinden Flecken und Schlupflöchern für zahlreiche Kriminelle und Terroristen führt, die in mehr als einem Mitgliedstaat agieren. **Aufgrund des grenzüberschreitenden Charakters der Bekämpfung der Kriminalität und der Verbesserung der Sicherheit können die Mitgliedstaaten die Informationslücke allein nicht schließen**. In diesem Bereich müssen sich die Mitgliedstaaten gegenseitig unterstützen.

Zwar arbeiten die Strafverfolgungsbehörden in der EU zusammen und tauschen Informationen aus, insbesondere über den durch die Prümer Beschlüsse (Beschlüsse 2008/615/JI und 2008/616/JI des Rates) geschaffenen Rahmen für den Austausch von Daten über DNA-Profile, Fingerabdrücke und Fahrzeugregister, aber es gibt erhebliche Schwachstellen.

Es gibt **vier zentrale Aspekte**, die die Strafverfolgungsbehörden bei der Bekämpfung der Kriminalität auf der Grundlage dieses Rahmens behindern und die sich alle auf die Suche nach und die Übermittlung von Informationen zwischen den Strafverfolgungsbehörden in der EU auswirken:

- 1) Die Strafverfolgungsbehörden sind nicht immer in der Lage **herauszufinden, ob Daten** über DNA-Profile, Fingerabdrücke oder Fahrzeugregister, die sie zur Erfüllung ihrer Aufgaben benötigen, **in der nationalen Datenbank eines anderen Mitgliedstaats verfügbar sind**.
- 2) Die Strafverfolgungsbehörden verfügen nicht über wirksame Mittel, um neben Daten über DNA-Profile, Fingerabdrücken und Fahrzeugregisterdaten, die in den nationalen Datenbanken anderer Mitgliedstaaten gespeichert sind und die sie zur Erfüllung ihrer Aufgaben benötigen, **andere sachdienliche Datenkategorien** abzufragen und darauf zuzugreifen.
- 3) Die Strafverfolgungsbehörden verfügen nicht über wirksame Mittel, um Daten über DNA-Profile, Fingerabdrücke und mögliche andere relevante Datenkategorien, die in der **Europol-Datenbank** gespeichert sind und die sie zur Erfüllung ihrer Aufgaben benötigen, abzufragen und darauf zuzugreifen.
- 4) Erhalten die Strafverfolgungsbehörden einen Hinweis darauf, dass Daten in der Datenbank eines anderen Mitgliedstaats vorhanden sind („Treffer“), haben sie nicht immer effizienten **Zugriff** auf die entsprechenden **tatsächlichen Daten**, die in der nationalen Datenbank dieses Mitgliedstaats gespeichert sind.

Diese vier miteinander verknüpften zentralen Aspekte stellen aufgrund ihrer Auswirkungen auf die wirksame Bekämpfung der Kriminalität und auf die Sicherheit und das Wohlergehen der EU-Bürgerinnen und -Bürger Probleme dar. Sie führen zu **wichtigen politischen Entscheidungen**, die eine detaillierte Bewertung der

¹ COM(2020) 605 final vom 24.7.2020.

Problemursachen, der damit verbundenen Ziele, der verfügbaren politischen Optionen und ihrer Auswirkungen erforderlich machen.

Was soll mit dieser Initiative erreicht werden?

Angesichts dringender operativer Erfordernisse und der Aufforderung des Rates, eine Überarbeitung der Prüm-Beschlüsse (Beschlüsse 2008/615/JI und 2008/616/JI des Rates) in Betracht zu ziehen, um deren Anwendungsbereich zu erweitern und die erforderlichen technischen und rechtlichen Anforderungen zu aktualisieren, soll diese Initiative den automatisierten Datenaustausch auf der Grundlage des Prüm-Rahmens verstärken und den Strafverfolgungsbehörden der Mitgliedstaaten bei der Bekämpfung der Kriminalität von Nutzen sein. Rechtsgrundlage für den Rechtsakt ist Artikel 82 Absatz 1 Unterabsatz 2 Buchstabe d und Artikel 87 Absatz 2 Buchstabe a des Vertrags über die Arbeitsweise der Europäischen Union (AEUV).

Als Reaktion auf die vier ermittelten Hauptprobleme sollen mit der Initiative die folgenden **Ziele** verwirklicht werden:

- 1) **Ziel I:** Bereitstellung einer technischen Lösung für einen **effizienten** automatisierten Datenaustausch zwischen den Strafverfolgungsbehörden der EU, um sie **auf einschlägige Daten hinzuweisen**, die in der nationalen Datenbank eines anderen Mitgliedstaats verfügbar sind,
- 2) **Ziel II:** Sicherstellung, dass allen zuständigen EU-Strafverfolgungsbehörden mehr **einschlägige Daten** (in Bezug auf die Datenkategorien) aus nationalen Datenbanken in anderen Mitgliedstaaten zur Verfügung stehen,
- 3) **Ziel III:** Sicherstellung, dass den Strafverfolgungsbehörden **einschlägige Daten** (in Bezug auf die Datenquellen) aus der **Europol**-Datenbank zur Verfügung stehen,
- 4) **Ziel IV:** Gewährleistung eines **effizienten Zugriffs** der Strafverfolgungsbehörden **auf die tatsächlichen Daten**, die einem „Treffer“ entsprechen und in der nationalen Datenbank eines anderen Mitgliedstaats oder bei Europol abrufbar sind.

Worin besteht der Mehrwert des Tätigwerdens auf EU-Ebene?

Aufgrund des grenzüberschreitenden Charakters der Bekämpfung der Kriminalität und der Sicherheitsfragen kann der Informationsaustausch in der Europäischen Union von den Mitgliedstaaten allein nicht ausreichend verbessert werden. In diesem Bereich müssen sich die Mitgliedstaaten gegenseitig unterstützen. Gemeinsame Vorschriften, Normen und Anforderungen auf EU-Ebene **erleichtern diesen Informationsaustausch** und sorgen gleichzeitig für **Kompatibilität** zwischen den verschiedenen nationalen Systemen. Dies wiederum ermöglicht eine gewisse Automatisierung der Arbeitsabläufe beim Informationsaustausch, die die Strafverfolgungsbehörden von arbeitsintensiven manuellen Tätigkeiten entlastet. Nicht zuletzt ermöglicht der Informationsaustausch auf EU-Ebene auch die Gewährleistung hoher Standards für **Datensicherheit** und **Datenschutz**.

B. Lösungen

Welche gesetzgeberischen und sonstigen Maßnahmen wurden erwogen? Wird eine Option bevorzugt? Warum?

Eine Reihe von gesetzgeberischen Optionen wurde in Betracht gezogen. Nach einer Vorauswahl wurden einige Optionen schnell wieder verworfen. Die anderen **politischen Optionen wurden eingehend untersucht**:

- 1) Politische Option für **Ziel I:** (*Bereitstellung einer technischen Lösung für einen **effizienten automatisierten Datenaustausch***)
 - **Politische Option 1.1:** Anwendung einer hybriden Lösung zwischen einem dezentralisierten und einem zentralisierten Ansatz ohne Datenspeicherung auf zentraler Ebene
- 2) Politische Optionen für **Ziel II:** (*Sicherstellung, dass den Strafverfolgungsbehörden mehr einschlägige Daten (in Bezug auf die **Datenkategorien**) zur Verfügung stehen*)
 - **Politische Option 2.1:** Aufnahme des Austauschs von Gesichtsbildern in den Prüm-Rahmen

- Politische Option 2.2: Aufnahme des Austauschs von Kriminalakten in den Prüm-Rahmen
- Politische Option 2.3: Aufnahme des Austauschs von Führerscheindaten in den Prüm-Rahmen

3) Politische Optionen für **Ziel III**: (*Sicherstellung, dass den Strafverfolgungsbehörden einschlägige Daten aus der Europol-Datenbank zur Verfügung stehen*)

- Politische Option 3.1: Ermöglichung der automatischen Überprüfung von Daten aus Drittländern durch die Mitgliedstaaten bei Europol als Teil des Prüm-Rahmens
- Politische Option 3.2: Ermöglichung des Abgleichs von Daten aus Drittländern mit den nationalen Datenbanken der Mitgliedstaaten durch Europol

4) Politische Optionen für **Ziel IV**: (*Gewährleistung eines **effizienten Zugriffs auf die tatsächlichen Daten**, die einem „Treffer“ entsprechen und in der nationalen Datenbank eines anderen Mitgliedstaats oder bei Europol verfügbar sind*)

- Politische Option 4.1: Regelung des Follow-up-Verfahrens auf EU-Ebene mit einem halbautomatischen Austausch von tatsächlichen Daten, die einem „Treffer“ entsprechen

Nach einer detaillierten Bewertung der Folgen der wichtigsten politischen Optionen setzt sich das **Paket der bevorzugten politischen Optionen** aus der politischen Option 1.1, den politischen Optionen 2.1 und 2.2, den politischen Optionen 3.1 und 3.2 und der politischen Option 4.1 zusammen.

Wer unterstützt welche Option?

Die Interessenträger befürworten im Allgemeinen den Ausbau des automatisierten Datenaustauschs auf der Grundlage des Prüm-Rahmens.

Die Mitgliedstaaten haben die bevorzugten politischen Optionen in mehreren Ratsgremien sowie in Schlussfolgerungen des Rates („Schlussfolgerungen des Rates 2018 zur Umsetzung der ‚PRÜMER-BESCHLÜSSE‘ zehn Jahre nach ihrer Annahme“) ausdrücklich unterstützt. Gleichzeitig sind sich die Mitgliedstaaten der Bedeutung ihrer nationalen Souveränität im Bereich der Strafverfolgung aus operativer und verfahrenstechnischer Sicht bewusst.

Das Europäische Parlament soll prüfen, ob die Notwendigkeit der Aufnahme einer neuen Datenkategorie in den Prüm-Rahmen gerechtfertigt ist und ob strenge Datenschutzgarantien vorhanden sind. Die Gespräche mit allen Interessenträgern haben gezeigt, wie wichtig es ist, angemessene Garantien zur Gewährleistung der Grundrechte und insbesondere des Rechts auf Schutz personenbezogener Daten vorzusehen.

C. Auswirkungen der bevorzugten Option

Was sind die Vorteile der bevorzugten Optionen (sofern vorhanden, ansonsten die wichtigsten)?

Das Paket der bevorzugten politischen Optionen (Option 1.1, Optionen 2.1 und 2.2, Optionen 3.1 und 3.2 sowie Option 4.1) würde eine wirksame Antwort auf die festgestellten Probleme darstellen und den derzeitigen Prüm-Rahmen durch **gezielte und starke zusätzliche Kapazitäten** ergänzen, um die Mitgliedstaaten bei der Intensivierung des Informationsaustauschs mit dem Endziel der **Verhütung und Ermittlung von terroristischen und anderen Straftaten** unter voller **Wahrung der Grundrechte stärker zu unterstützen**.

Alle **bevorzugten Optionen kommen letztlich den Bürgerinnen und Bürgern zugute**, die direkt und indirekt von einer besseren Bekämpfung der Kriminalität und niedrigeren Kriminalitätsraten profitieren werden. Im Hinblick auf die Effizienz **sind die nationalen Strafverfolgungsbehörden die Hauptnutznießer**. Die bevorzugten politischen Optionen bieten effiziente Lösungen für Herausforderungen, die andernfalls mit höheren Kosten oder weniger effizient angegangen werden müssten.

Welche Kosten entstehen bei den bevorzugten Optionen (sofern vorhanden, ansonsten die wichtigsten)?

Die bevorzugten politischen Optionen erfordern Investitionen sowohl auf EU-Ebene als auch auf Ebene der

Mitgliedstaaten. Die Investitionskosten auf nationaler Ebene betragen einmalig 4,4 Mio. EUR und jährlich 882 000 EUR. Auf EU-Ebene belaufen sich die Investitionskosten auf einmalig 17,17 Mio. EUR und jährlich 4,1 Mio. EUR. Dabei handelt es sich um geschätzte Beträge, die auf früheren Erfahrungen mit der Entwicklung und Umsetzung von IT-Infrastrukturen auf EU-Ebene beruhen. Einige der politischen Optionen lassen sich jedoch nur schwer genau beziffern. Es wird davon ausgegangen, dass die voraussichtlichen Investitionskosten durch Vorteile und Einsparungen, insbesondere auf Ebene der Mitgliedstaaten, aufgewogen werden. Die Einrichtung des zentralen Prümer Routers wird den Mitgliedstaaten Kosten ersparen, da sie nicht so viele Verbindungen herstellen müssen, wie es Mitgliedstaaten und Datenkategorien gibt.

Die bevorzugten politischen Optionen werden voraussichtlich keine Auswirkungen auf kleine und mittlere Unternehmen haben. Die bevorzugten Optionen enthalten keine regulatorischen Pflichten für Bürgerinnen und Bürger oder Verbraucher und verursachen daher keine zusätzlichen Kosten für diese Interessenträger.

Worin bestehen die Auswirkungen auf Unternehmen, KMU und Kleinunternehmen?

Die bevorzugten politischen Optionen dürften keine nennenswerten Auswirkungen auf Unternehmen haben.

Wird es spürbare Auswirkungen auf nationale Haushalte und Behörden geben?

Wie bereits erwähnt, belaufen sich die voraussichtlichen Investitionskosten auf nationaler Ebene auf einmalig 4,4 Mio. EUR und jährlich auf 882 000 EUR, die durch Haushaltseinsparungen ausgeglichen werden, die sich aus der Nutzung des zentralen Routers anstelle von so vielen nationalen Verbindungen für jeden Mitgliedstaat, wie es Mitgliedstaaten und Datenkategorien gibt, ergeben. Den Schätzungen zufolge könnten die kumulierten Haushaltseinsparungen auf nationaler Ebene die Anfangsinvestitionen sowohl auf zentraler als auch auf nationaler Ebene binnen zwei Jahren ausgleichen.

Gibt es andere nennenswerte Auswirkungen?

Alle bevorzugten Optionen betreffen die Verarbeitung von personenbezogenen Daten. Folglich haben diese politischen Optionen Auswirkungen auf die Grundrechte und insbesondere auf das Recht auf Schutz personenbezogener Daten (Artikel 8 der Charta) und auf Achtung des Privat- und Familienlebens (Artikel 7 der Charta). Im Hinblick auf die vollständige Einhaltung der Grundrechte wird in der Folgenabschätzung eine **gründliche Berücksichtigung der Grundrechte** während der gesamten Analyse vorgesehen. Somit stehen alle bevorzugten politischen Optionen im Einklang mit einem **grundlegenden Ziel** und sind **streng auf das beschränkt, was** zur Erreichung dieses Ziels **erforderlich und verhältnismäßig ist**.

D. Folgemaßnahmen

Wann wird die Maßnahme überprüft?

Vier Jahre, nachdem die neuen Funktionen eingerichtet und in Betrieb genommen wurden, und danach alle vier Jahre, sollten die Mitgliedstaaten und die Agenturen der Union dem Europäischen Parlament, dem Rat und der Kommission einen Bericht über die **technische Funktionsweise** der vorgeschlagenen neuen Maßnahmen vorlegen. Darüber hinaus sollte die Kommission ein Jahr nach Vorlage dieser Berichte durch die Mitgliedstaaten und die Agenturen der Union eine **Gesamtbewertung** der Maßnahmen vornehmen und dabei auch die direkten und indirekten **Auswirkungen auf die Grundrechte** untersuchen. Darin sollten die Ergebnisse an den Zielen gemessen werden, und es sollte beurteilt werden, ob die grundlegenden Prinzipien weiterhin Gültigkeit haben; außerdem sollten etwaige Schlussfolgerungen für künftige Optionen gezogen werden. Die Kommission sollte dem Europäischen Parlament und dem Rat die Bewertungsberichte vorlegen.