



Brüssel, den 8.12.2021  
SWD(2021) 377 final

**ARBEITSUNTERLAGE DER KOMMISSIONSDIENSTSTELLEN**  
**BERICHT ÜBER DIE FOLGENABSCHÄTZUNG (ZUSAMMENFASSUNG)**

*Begleitunterlage zum*

**Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates**  
**über den Informationsaustausch zwischen Strafverfolgungsbehörden der**  
**Mitgliedstaaten und zur Aufhebung des Rahmenbeschlusses 2006/960/JI des Rates**

{COM(2021) 782 final} - {SEC(2021) 420 final} - {SWD(2021) 374 final}

## Zusammenfassung

### Folgenabschätzung zu einem Vorschlag zur Modernisierung der bestehenden Zusammenarbeit auf dem Gebiet der Strafverfolgung innerhalb der EU durch die Schaffung eines EU-Kodexes für die polizeiliche Zusammenarbeit im Bereich Informationsaustausch und Kommunikation

#### A. Handlungsbedarf

##### Warum? Um welche Problematik geht es?

Sicherheit und grenzüberschreitende Kriminalität (einschließlich Steuerstraftaten) sind definitionsgemäß ein internationales Problem. Wie in der EU-Strategie für eine Sicherheitsunion von 2020 ausgeführt ist, erlebt Europa heute ein **sich wandelndes Sicherheitsumfeld**, das durch immer neue und komplexere Sicherheitsbedrohungen gekennzeichnet ist. Diese Bedrohungen machen an Grenzen nicht Halt und manifestieren sich in organisierten kriminellen Vereinigungen, die an einem breiten Spektrum krimineller Aktivitäten beteiligt sind. Selbst ein vermeintlich auf die lokale Ebene beschränktes Verbrechen kann Verbindungen zu anderen Straftaten haben, die in ganz Europa von denselben Tätern begangen werden. Darüber hinaus bringt die **zunehmende Mobilität innerhalb der EU** zusätzliche Herausforderungen für die Prävention und Bekämpfung aller Formen krimineller Bedrohungen mit sich.

Die sich **rasch wandelnde kriminelle Landschaft und die zunehmende Mobilität der Menschen** deuten darauf hin, dass die grenzüberschreitende Zusammenarbeit zwischen den Strafverfolgungsbehörden in der EU von entscheidender Bedeutung sein wird, um Straftaten zu bekämpfen und es den EU-Bürgerinnen und -Bürgern zu ermöglichen, ihr Recht auf Freizügigkeit in Zukunft sicher wahrzunehmen.

Allerdings gibt es nach wie vor Grenzen und Hindernisse für den Datenaustausch zwischen den Strafverfolgungsbehörden, was zur Folge hat, dass zahlreiche Kriminelle und Terroristen, die in mehr als einem Mitgliedstaat agieren, blinde Flecken und Schlupflöcher für sich nutzen. Angesichts des grenzüberschreitenden Charakters der Kriminalitätsbekämpfung und der Verbesserung der Sicherheit müssen sich die Mitgliedstaaten aufeinander verlassen können, um die Informationslücke zu schließen.

Die Strafverfolgungsbehörden in der EU arbeiten zusammen und tauschen Informationen aus, insbesondere auf der Grundlage des Rahmenbeschlusses (2006/960/JI) über die Vereinfachung des Austauschs von Informationen und Erkenntnissen zwischen den Strafverfolgungsbehörden der Mitgliedstaaten der Europäischen Union (schwedischer Rahmenbeschluss), es bestehen jedoch noch bedeutende Mängel.

Es gibt **drei rechtliche, strukturelle und technische Kernprobleme**, aufgrund derer die Strafverfolgungsbehörden heute **weder wirksam noch effizient** mit ihren Partnern in anderen Mitgliedstaaten **Informationen austauschen**.

- 1) **Vorschriften auf nationaler Ebene behindern einen wirksamen und effizienten Informationsfluss.** Der schwedische Rahmenbeschluss von 2006 wird nicht vollständig umgesetzt, wodurch die Strafverfolgungsbehörden anderer Mitgliedstaaten solche Informationen nicht in wirksamer und effizienter Weise erhalten.
- 2) **Die Strukturen auf nationaler Ebene sind nicht immer hinreichend effizient und wirksam eingerichtet und ausgestattet.** Die Mitgliedstaaten verfügen nicht immer über die erforderlichen Strukturen, um Informationensuchen von anderen Mitgliedstaaten entgegenzunehmen, sie an die richtigen Behörden auf nationaler Ebene weiterzuleiten und die angeforderten Informationen entsprechend bereitzustellen.
- 3) **Die freie Wahl des Kommunikationskanals/der Kommunikationskanäle zwischen den Mitgliedstaaten führt immer wieder zu doppelten Ersuchen.** Die Strafverfolgungsbehörden der Mitgliedstaaten nutzen eine Vielzahl unterschiedlicher Kanäle, um Informationensuchen an andere Mitgliedstaaten zu richten und diese zu beantworten, was einen wirksamen und effizienten Informationsaustausch behindert.

Diese drei Probleme sind miteinander verknüpft. Alle drei erfordern wichtige politische Entscheidungen, die eine detaillierte Bewertung der Problemursachen, der damit verbundenen Ziele, der verfügbaren politischen Optionen und ihrer Auswirkungen notwendig machen.

##### Was soll mit dieser Initiative erreicht werden?

Von dieser Initiative wird erwartet, dass die Mitgliedstaaten bei der Erfüllung ihrer Verpflichtung zur Zusammenarbeit auf dem Gebiet der Strafverfolgung grundlegend unterstützt werden. Den dringenden

operativen Erfordernissen wird Rechnung getragen und der Rat wird aufgefordert, die „Konsolidierung des EU-Rechtsrahmens zur weiteren Stärkung der grenzüberschreitenden Zusammenarbeit bei der Strafverfolgung, zur Unterstützung der Entwicklung eines reibungslosen und raschen Informationsaustauschs und der Weiterentwicklung der einschlägigen Strukturen und Plattformen zu unterstützen“.

Mit der Initiative sollen folgende **Ziele** erreicht werden:

- 1) Ziel I: Erleichterung eines **gleichwertigen Zugangs der Strafverfolgungsbehörden** zu Informationen, die in einem anderen Mitgliedstaat verfügbar sind (vergleichbar mit dem Zugang zu Informationen innerhalb eines Mitgliedstaates), unter Wahrung der Grundrechte und der Datenschutzanforderungen
- 2) Ziel II: Sicherstellung, dass alle Mitgliedstaaten über eine wirksam funktionierende **zentrale Kontaktstelle** (Single Point of Contact, SPOC) verfügen, einschließlich der Fälle, in denen eine **richterliche Genehmigung** für die Bereitstellung der Daten auf Ersuchen eines anderen Mitgliedstaats erforderlich ist, und Gewährleistung einer wirksamen Zusammenarbeit mit den **Zentren für die Zusammenarbeit von Polizei und Zoll** (Police and Customs Cooperation Centres, PCCC)
- 3) Ziel III: Einrichtung eines **obligatorischen Standard-Kommunikationskanals** für den Austausch strafverfolgungsrelevanter Informationen zwischen den Mitgliedstaaten (sofern relevant)

### **Worin besteht der Mehrwert des Tätigwerdens auf EU-Ebene?**

Die EU-Maßnahmen dürften der gesamten EU zugutekommen und sich auch auf die assoziierten Schengen-Länder auswirken, indem sie die Sicherheit und das Vertrauen zwischen den Mitgliedstaaten insgesamt stärken. Damit soll das Grundprinzip des Schengen-Raums (ein Raum ohne Kontrollen an den Binnengrenzen) unterstützt werden.

Gemeinsame **Vorschriften, Mindeststandards und Anforderungen auf EU-Ebene** werden den Informationsfluss im Einklang mit **hohen Standards für Datensicherheit und Datenschutz** erheblich verbessern.

Darüber hinaus ermöglichen gemeinsame Standards eine gewisse Automatisierung der Arbeitsabläufe beim Informationsaustausch, wodurch die Strafverfolgungsbeamten von bestimmten arbeitsintensiven/zeitaufwendigen manuellen Tätigkeiten entlastet werden.

## **B. Lösungen**

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

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

- 1) Politische Optionen für **Ziel I**: (*Erleichterung des gleichwertigen Zugangs zu Informationen*)
  - Politische Option 1.1: Legislativvorschlag zur Aktualisierung des schwedischen Rahmenbeschlusses von 2006 zur Gewährleistung seiner Angleichung an die Richtlinie zum Datenschutz bei der Strafverfolgung von 2016 sowie flankierende „weiche“ Maßnahmen (Schulungen, Leitlinien der Kommission)
  - Politische Option 1.2: Option 1.1 sowie Vereinfachung der Nutzung des schwedischen Rahmenbeschlusses sowie mehr Klarheit über die für einen möglichen Austausch verfügbaren nationalen Datensätze
  - Politische Option 1.3: Option 1.2 sowie Bestimmungen, die die Einhaltung der Fristen gewährleisten, innerhalb derer Daten einem anderen Mitgliedstaat zur Verfügung zu stellen sind (auch in den Fällen, in denen eine richterliche Genehmigung erforderlich ist)
- 2) Politische Optionen für **Ziel II**: (*Sicherstellung, dass alle Mitgliedstaaten über eine wirksam funktionierende zentrale Kontaktstelle (Single Point of Contact, SPOC) verfügen, einschließlich der Fälle, in denen eine richterliche Genehmigung für die Bereitstellung der Daten auf Ersuchen eines anderen Mitgliedstaats erforderlich ist, und Gewährleistung einer wirksamen Zusammenarbeit mit den Zentren für die Zusammenarbeit von Polizei und Zoll (Police and Customs Cooperation Centres, PCCC)*)
  - Politische Option 2.1: Weiterführung der unverbindlichen Leitlinien des Rates zu nationalen zentralen Kontaktstellen sowie flankierenden „weichen“ Maßnahmen (Schulungen, finanzielle

Unterstützung, Leitlinien)

- Politische Option 2.2: Angleichung der Mindeststandards für die Zusammensetzung der zentralen Kontaktstellen (einschließlich der obligatorischen Präsenz einer Justizbehörde), ihre Aufgaben, Personalausstattung und IT-Systeme sowie in Bezug auf ihre Zusammenarbeit mit regionalen Strukturen wie Zentren für die Zusammenarbeit von Polizei und Zoll sowie flankierende „weiche“ Maßnahmen (Schulungen, finanzielle Unterstützung, Leitlinien)
- Politische Option 2.3: Harmonisierung der Vorschriften über die Zusammensetzung der zentralen Kontaktstellen (einschließlich der obligatorischen Präsenz einer Justizbehörde), ihre Aufgaben, Personalausstattung und IT-Systeme sowie in Bezug auf ihre Zusammenarbeit mit regionalen Strukturen wie Zentren für die Zusammenarbeit von Polizei und Zoll sowie flankierende „weiche“ Maßnahmen (Schulungen, finanzielle Unterstützung, Leitlinien)

3) Politische Optionen für **Ziel III**: *(Einrichtung eines obligatorischen Standard-Kommunikationskanals für den Austausch strafverfolgungsrelevanter Informationen zwischen den Mitgliedstaaten (sofern relevant))*

- Politische Option 3.1: Weiterführung der unverbindlichen Leitlinien und Empfehlungen des Rates, um Europol bei der Nutzung von SIENA<sup>1</sup> in Fällen, die in den Zuständigkeitsbereich von Europol fallen, in Kopie zu setzen, sowie flankierende „weiche“ Maßnahmen (Schulungen, finanzielle Unterstützung)
- Politische Option 3.2: Verpflichtung zur Nutzung desselben Kommunikationskanals für denselben Zweck (wobei SIENA von Europol gegebenenfalls der bevorzugte Kanal ist) sowie Verpflichtung, Europol bei der Nutzung von SIENA in Fällen, die in den Zuständigkeitsbereich von Europol fallen, in Kopie zu setzen, sowie flankierende „weiche“ Maßnahmen (wie in Option 3.1)
- Politische Option 3.3: Verpflichtung zur standardmäßigen Verwendung von SIENA für den gesamten bilateralen Informationsaustausch (sofern nicht anderweitig durch EU-Recht geregelt) sowie Verpflichtung, Europol in Fällen, die in den Zuständigkeitsbereich von Europol fallen, in Kopie zu setzen – es gilt ein Übergangszeitraum, und für die Einführung von SIENA wird Unterstützung aus dem Fonds für die innere Sicherheit geleistet – sowie flankierende Maßnahmen (wie in Option 3.1)

Nach einer detaillierten Bewertung der Folgen der wichtigsten politischen Optionen setzt sich das **Paket der bevorzugten politischen Optionen** aus der **politischen Option 1.3, der politischen Option 2.2 und der politischen Option 3.3** zusammen.

#### Wer unterstützt welche Option?

Die Interessenträger befürworten im Allgemeinen die die Verbesserung eines reibungslosen und zeitnahen Informationsaustauschs und den weiteren Ausbau der entsprechenden Strukturen und Plattformen.

Von den Mitgliedstaaten wird erwartet, dass sie die meisten der im Rahmen der bevorzugten Option geplanten Maßnahmen unterstützen. Gleichzeitig sind sich die Mitgliedstaaten der Bedeutung ihrer nationalen Souveränität im Bereich der Strafverfolgung aus operativer und verfahrenstechnischer Sicht bewusst. Auf Expertenebene geäußerte positive Meinungen werden möglicherweise auf politischer Ebene nicht weiter geteilt.

Der wahrscheinlich wichtigste Diskussionspunkt betrifft Option 3.3 (standardmäßige Verwendung der Europol-Anwendung SIENA als obligatorischer Kanal für die Kommunikation zwischen den Mitgliedstaaten (sofern nicht anderweitig durch EU-Recht geregelt)). Diese Option wurde jedoch auch von den Mitgliedstaaten im Rat verteidigt: „Die Anwendung von SIENA als Standard-Kommunikationskanal würde zur Straffung des Informationsaustauschs zwischen den Strafverfolgungsbehörden beitragen und das Sicherheitsniveau im Rahmen der polizeilichen Zusammenarbeit in der Europäischen Union erhöhen. Gleichzeitig wäre es möglich, die Bemühungen auf die Entwicklung einer einzigen statt zahlreicher Lösungen zu konzentrieren und damit das Ziel zu fördern, die innere Sicherheit in der EU zu verbessern“.

Es wird erwartet, dass das Europäische Parlament das Vorhandensein strenger Datenschutzgarantien prüft. Die Gespräche mit allen Interessenträgern haben gezeigt, wie wichtig angemessene Garantien zur Gewährleistung der Grundrechte und insbesondere des Rechts auf den Schutz personenbezogener Daten sind.

<sup>1</sup> Europol's Netzanwendung für sicheren Datenaustausch (Secure Information Exchange Network Application).

## C. Auswirkungen der bevorzugten Option

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

Die bevorzugte Option, die als bahnbrechende Neuerung gelten kann, wäre eine wirksame Antwort auf die festgestellten Probleme und würde gleichzeitig die Unterstützung der Mitgliedstaaten durch Europol verstärken, mit dem Ziel, **Straftaten zu verhüten, aufzudecken und zu untersuchen**, unter uneingeschränkter **Wahrung der Grundrechte**.

**Die Nutznießer der bevorzugten Option sind letztendlich die Bürgerinnen und Bürger.** Sie sind es, die direkt und indirekt von einer besseren Kriminalitätsbekämpfung und niedrigeren Kriminalitätsraten profitieren werden. Im Hinblick auf die Effizienz sind die **nationalen Strafverfolgungsbehörden die Hauptnutznießer**.

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

Die bevorzugte Option erfordert Investitionen sowohl auf EU-Ebene als auch auf Ebene der Mitgliedstaaten. Diese Kosten würden im Wesentlichen IT-Aufrüstungen und Schulungen betreffen. Die Investitionen wären von Mitgliedstaat zu Mitgliedstaat sehr unterschiedlich und hängen von der Effizienz und Effektivität der nationalen zentralen Kontaktstellen und der Zentren für die Zusammenarbeit von Polizei und Zoll (falls vorhanden) ab.

Die bevorzugte Option bietet effiziente Lösungen für Herausforderungen, die andernfalls mit höheren Kosten verbunden wären, eine schlechte Kompatibilität aufwiesen oder weniger effizient wären.

Einige der Optionen sind jedoch schwer zu quantifizieren. Nach Angaben von Europol werden die Kosten für die Integration der Europol-Anwendung SIENA in die Fallbearbeitungssysteme (CMS) von 20 Mitgliedstaaten und die Entwicklung von CMS in 10 Mitgliedstaaten auf 2,5 Mio. EUR geschätzt (einmalig erforderliche Investition). Durch die Verbesserung der Effizienz würden diese Kosten jedoch aufgewogen (weniger Ressourcen für die Fallbearbeitung, d. h. mehr Ressourcen für die „Lösung von Fällen“).

Die bevorzugte Option enthält keine regulatorischen Verpflichtungen für Bürgerinnen und Bürger oder Verbraucher und verursacht für diese Interessenträger daher auch keine zusätzlichen Kosten.

### Worin bestehen die Auswirkungen auf Unternehmen, KMU und Kleinstunternehmen?

Die bevorzugte Option könnte angesichts der gestiegenen Nachfrage nach IT-Produkten und -Dienstleistungen geringe positive Auswirkungen auf kleine und mittlere Unternehmen haben.

### Wird es nennenswerte Auswirkungen auf nationale Haushalte und Behörden geben?

Wie bereits erwähnt, erfordert die bevorzugte Option Investitionen auf Ebene der Mitgliedstaaten. Diese Kosten würden im Wesentlichen IT-Aufrüstungen und Schulungen betreffen. Einige der Optionen sind jedoch schwer zu quantifizieren. Diese Kosten wären von Mitgliedstaat zu Mitgliedstaat sehr unterschiedlich und hängen von der Effizienz und Effektivität der nationalen zentralen Kontaktstellen und der Zentren für die Zusammenarbeit von Polizei- und Zollbehörden (falls vorhanden) ab.

Nach Angaben von Europol könnten sich die Kosten für die Entwicklung eines Fallbearbeitungssystems auf nationaler Ebene auf 150 000 EUR (einmalig) pro Mitgliedstaat belaufen. Durch die Verbesserung der Effizienz würden diese Kosten jedoch aufgewogen (weniger Ressourcen für die Fallbearbeitung, d. h. mehr Ressourcen für die „Lösung von Fällen“).

Die Kosten für die notwendigen IT-Aufrüstungen sowohl in den SPOC als auch in den PCCC könnten sich auf insgesamt maximal **11,5 Mio. EUR** belaufen (2,5 Mio. EUR für SPOC und 9 Mio. EUR für PCCC).

Diese als akzeptabel erachteten Kosten (einmalige Investition) **stehen in einem angemessenen Verhältnis** zu dem festgestellten Problem und gehen nicht über das zur Erreichung des spezifischen Ziels erforderliche Maß hinaus. Unterstützung wird aus dem EU-Fonds für die innere Sicherheit geleistet werden (im Wesentlichen über nationale Programme).

### Wird es andere nennenswerte Auswirkungen geben?

Durch die bevorzugte Option werden die nationalen und regionalen Informationszentren der Mitgliedstaaten in die Lage versetzt, den Zugang zu vorhandenen Daten und deren Austausch wirksamer und effizienter zu gestalten.

Die bevorzugte Option gewährleistet auch die vollständige Angleichung einer neuen Richtlinie über den Informationsaustausch und die Kommunikation an die Richtlinie zum Datenschutz bei der Strafverfolgung von 2016. Eine solche Angleichung gewährleistet eine ausdrückliche Einhaltung der Grundrechte, was derzeit beim schwedischen Rahmenbeschluss von 2006 nicht der Fall ist.

Die bevorzugte Option entspricht einem **Ziel von allgemeinem Interesse** und ist **strikt auf das beschränkt, was** zur Erreichung dieses Ziels **notwendig und verhältnismäßig** ist.

#### **D. Folgemaßnahmen**

##### **Wann wird die Maßnahme überprüft?**

**[Zwei]** Jahre nach Ablauf der Umsetzungsfrist und danach alle **[vier]** Jahre sollte die Kommission dem Europäischen Parlament und dem Rat zwei Berichte vorlegen. **Der erste Bericht** sollte darlegen, inwieweit die Mitgliedstaaten die erforderlichen Maßnahmen zur Umsetzung dieser Richtlinie ergriffen haben. **Der zweite Bericht** sollte die Ergebnisse an den Zielen messen, und es sollte beurteilt werden, ob die grundlegenden Prinzipien weiterhin Gültigkeit haben; außerdem sollten etwaige Schlussfolgerungen für künftige Optionen gezogen werden.