

Brüssel, den 5.2.2019  
COM(2019) 70 final

ANNEX

## **ANHANG**

**der**

### **Empfehlung für einen BESCHLUSS DES RATES**

**über die Ermächtigung zur Aufnahme von Verhandlungen über ein Abkommen  
zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über den  
grenzüberschreitenden Zugang zu elektronischen Beweismitteln für die justizielle  
Zusammenarbeit in Strafsachen**

## ANHANG

### **1. ZIELE**

Die Kommission sollte in den Verhandlungen die nachstehend im Einzelnen beschriebenen besonderen Ziele anstreben, gleichzeitig jedoch sicherstellen, dass das Verhandlungsergebnis mit den internen Vorschriften der Union zu elektronischen Beweismitteln in ihrer jeweiligen Fassung während des Gesetzgebungsverfahrens der beiden gesetzgebenden Organe der Union und schließlich in ihrer verabschiedeten endgültigen Fassung vereinbar ist. Diese internen Vorschriften dienen als Ausgangspunkt für die Verhandlungsposition der Union.

1. Festlegung gemeinsamer Vorschriften für Anordnungen zur Beschaffung elektronischer Beweismittel in Form von Inhalts- und Nichtinhaltsdaten, die eine Justizbehörde in einer Vertragspartei an einen dem Recht einer anderen Vertragspartei unterliegenden Diensteanbieter richtet, und Bewältigung diesbezüglicher Rechtskollisionen. Dies dürfte die Gefahr einer Fragmentierung der Verfahren und Rechtsvorschriften verringern und die Rechtssicherheit im Verhältnis zwischen der Union und den Vereinigten Staaten von Amerika bei der Beschaffung elektronischer Beweismittel in Strafverfahren erhöhen.
2. Ermöglichung der gegenseitigen direkten Übermittlung elektronischer Beweismittel von einem Diensteanbieter an eine ersuchende Behörde nach Nummer 1.
3. Sicherstellung der Beachtung der Grundrechte, Grundfreiheiten und allgemeinen Grundsätze des Unionsrechts, wie sie in den Verträgen und der Charta der Grundrechte der Europäischen Union verankert sind, darunter die Verhältnismäßigkeit, die Verfahrensrechte, die Unschuldsvermutung und die Verteidigungsrechte von Personen, gegen die ein Strafverfahren anhängig ist, sowie die Privatsphäre und der Schutz von personenbezogenen Daten und Kommunikationsdaten bei der Verarbeitung dieser Daten, einschließlich der Übermittlung an Strafverfolgungsbehörden in Drittstaaten, und etwaige diesbezügliche Pflichten der Strafverfolgungs- und Justizbehörden.

Um die in Abschnitt 1 beschriebenen Ziele zu erreichen, sollte in dem Abkommen insbesondere Folgendes geregelt werden:

### **2. ART UND ANWENDUNGSBEREICH DES ABKOMMENS**

4. Das Abkommen sollte auf Strafverfahren Anwendung finden, die sowohl ein Vor- als auch ein Hauptverfahren umfassen.
5. Das Abkommen sollte gegenseitige Rechte und Pflichten für die Vertragsparteien begründen.
6. Im Abkommen sollten die Definitionen und die Arten der betroffenen Daten (sowohl Inhalts- als auch Nichtinhaltsdaten) festgelegt werden.
7. Im Abkommen sollten sein genauer Anwendungsbereich in Bezug auf die erfassten Straftaten und die Schwellenwerte festgelegt werden.
8. Im Abkommen sollte festgelegt werden sollte, welche Voraussetzungen erfüllt sein müssen, damit eine Justizbehörde eine Anordnung erlassen kann, und wie eine Anordnung befolgt werden kann.

9. Das Abkommen sollte eine Klausel enthalten, die wirksame gerichtliche Rechtsbehelfe für betroffene Personen während des Strafverfahrens ermöglicht. Ferner sollte im Abkommen festgelegt werden, unter welchen Umständen ein Diensteanbieter das Recht hat, einer Anordnung zu widersprechen.
10. Im Abkommen sollte eine Frist für die Bereitstellung der von der Anordnung erfassten Daten festgelegt werden.
11. Das Abkommen sollte andere bestehende internationale Abkommen über justizielle Zusammenarbeit in Strafsachen zwischen Behörden, wie das Rechtshilfeabkommen zwischen der EU und den USA, unberührt lassen.
12. Das Abkommen sollte in den bilateralen Beziehungen zwischen der Union und den Vereinigten Staaten von Amerika Vorrang vor dem Übereinkommen des Europarats über Computerkriminalität und Übereinkünften oder Regelungen haben, die in den Verhandlungen über das Zweite Zusatzprotokoll zum Übereinkommen des Europarats über Computerkriminalität vereinbart werden, soweit die Bestimmungen dieser Übereinkünfte oder Regelungen Fragen betreffen, die in dem Abkommen behandelt werden.

### **3. GARANTIEN**

13. Das Abkommen sollte in Bezug auf die Kategorien von Personen, um deren Daten nach diesem Abkommen nicht ersucht werden darf, auf Gegenseitigkeit beruhen. Das Abkommen sollte nicht zu einer Diskriminierung zwischen Personen aus verschiedenen Mitgliedstaaten führen.
14. Das Abkommen sollte durch Bezugnahme auf das am 1. Februar 2017 in Kraft getretene Datenschutzabkommen zwischen der EU und den USA (auch als „Rahmenabkommen“ bekannt) anwendbar gemacht werden.
15. Das Abkommen sollte das Rahmenabkommen durch zusätzliche Garantien ergänzen, die der Sensibilität der betroffenen Datenkategorien und den besonderen Anforderungen an die direkte Übermittlung elektronischer Beweismittel durch Diensteanbieter statt zwischen Behörden Rechnung tragen.
16. Zu den zusätzlichen Garantien für den Schutz der Privatsphäre und den Datenschutz, die im Rahmen des Anwendungsbereichs des Abkommens zu überprüfen sind, sollten unter anderem gehören:
  - a) Die Angabe der Zwecke, für die personenbezogene Daten und elektronische Kommunikationsdaten angefordert und übermittelt werden dürfen.
  - b) Die Bestimmung, dass die Anordnung auf die personenbezogenen Daten und elektronischen Kommunikationsdaten beschränkt werden muss, die für die Zwecke, für die auf sie zugegriffen wird, erforderlich und angemessen sind.
  - c) Die Bestimmung, dass für die Verwendung durch und die Offenlegung gegenüber US-Behörden, die nicht durch das Rahmenabkommen gebunden sind, die Benachrichtigung und die vorherige Genehmigung der zuständigen Justizbehörde erforderlich ist, die in dem Mitgliedstaat benannt ist, in dem der Diensteanbieter niedergelassen oder vertreten ist, und dass eine solche Verwendung oder Offenlegung nur stattfinden darf, wenn gewährleistet ist, dass die empfangende Behörde die personenbezogenen Daten und elektronischen Kommunikationsdaten im Einklang mit den Bestimmungen des Abkommens wirksam schützt. Bei der Prüfung einer solchen vorherigen

Genehmigung sollte die zuständige Justizbehörde alle relevanten Umstände gebührend berücksichtigen, etwa die Schwere der Straftaten und den Zweck, für den die Daten ursprünglich übermittelt wurden.

- d) Die Bestimmung, dass eine Weiterübermittlung an andere Drittstaaten nur an Strafverfolgungsbehörden erfolgen darf, die für die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten einschließlich Terrorismus zuständig sind, und dass für eine solche Weiterübermittlung die Benachrichtigung und die vorherige Genehmigung der zuständigen Justizbehörde erforderlich sein sollte, die von dem Mitgliedstaat benannt ist, in dem der Diensteanbieter niedergelassen oder vertreten ist. Bei der Prüfung einer solchen vorherigen Genehmigung sollte die zuständige Justizbehörde die in Artikel 7 Absatz 2 des Rahmenabkommens genannten Umstände berücksichtigen.
- e) Das Abkommen kann sich mit den außergewöhnlichen Umständen und den Garantien befassen, die notwendig sind, wenn die Weiterübermittlung im Falle einer ernststen, unmittelbar drohenden Gefahr für die öffentliche Sicherheit eines Mitgliedstaats oder eines Drittstaats ohne vorherige Genehmigung erfolgen kann.
- f) Die Meldung eines Datensicherheitsvorfalls an die zuständige Behörde, die von dem Mitgliedstaat benannt ist, in dem der Diensteanbieter niedergelassen oder vertreten ist, sollte unter den Bedingungen des Artikels 10 Absatz 2 des Rahmenabkommens erfolgen.

17. Zu den zusätzlichen verfahrensrechtlichen Garantien, die im Rahmen des Anwendungsbereichs des Abkommens zu überprüfen sind, sollten unter anderem gehören:

- a) Geeignete Garantien, um sicherzustellen, dass um Daten nicht für die Verwendung in Strafverfahren ersucht werden darf, die zur Verhängung der Todesstrafe führen könnten.
- b) Angemessene Bedingungen, um die Erforderlichkeit und Angemessenheit der Anordnungen für den Zugang zu elektronischen Beweismitteln sicherzustellen, wobei gegebenenfalls insbesondere zwischen Datenkategorien unterschieden wird.
- c) Verfahrensgarantien für Personen, die Gegenstand einer Datenanordnung im Rahmen eines Strafverfahrens sind.
- d) Besondere Garantien für Daten, die durch Vorrechte und Immunitäten geschützt sind.
- e) Vertraulichkeitsgarantien für Behörden und Diensteanbieter, unter anderem Verbot der Offenlegung.

#### **4. GOVERNANCE DES ABKOMMENS**

18. Das Abkommen sollte vorsehen, dass die Vertragsparteien eine regelmäßige gemeinsame Überprüfung der Anwendung des Abkommens vornehmen und prüfen, wie es möglichst wirksam genutzt werden kann. Zu diesem Zweck sollten auf beiden Seiten statistische Daten erhoben werden, um diesen Prozess zu erleichtern.

19. Das Abkommen sollte eine Klausel über seine Laufzeit enthalten. Ob es auf unbestimmte Zeit oder für eine befristete Laufzeit geschlossen werden sollte, ist unter Berücksichtigung der Verhandlungsergebnisse zu prüfen. In jedem Fall sollte eine Bestimmung in das Abkommen aufgenommen werden, die seine Überprüfung zu gegebener Zeit vorschreibt.
20. Im Abkommen sollte vorgesehen werden, dass die Vertragsparteien einander konsultieren sollten, um die Beilegung von Streitigkeiten über die Auslegung oder die Anwendung des Abkommens zu erleichtern.
21. Das Abkommen sollte die Möglichkeit der Aussetzung oder Kündigung des Abkommens durch eine Vertragspartei für den Fall vorsehen, dass die Streitigkeit in dem genannten Konsultationsverfahren nicht beigelegt werden kann
22. Das Abkommen sollte eine Klausel über seinen räumlichen Anwendungsbereich enthalten.
23. Das Abkommen wird in allen Amtssprachen der Union gleichermaßen verbindlich sein.