EUROPÄISCHE
KOMMISSION

Brüssel, den 13.5.2022
COM(2022) 208 final

ANNEX

ANHANG

des

Vorschlags für einen

BESCHLUSS DES RATES

über den Abschluss des Abkommens zwischen der Europäischen Union einerseits und Neuseeland andererseits über den Austausch personenbezogener Daten zwischen der Agentur der Europäischen Union für die Zusammenarbeit auf dem Gebiet der Strafverfolgung (Europol) und den für die Bekämpfung von schwerer Kriminalität und Terrorismus zuständigen neuseeländischen Behörden

ANHANG

DIE EUROPÄISCHE UNION, nachstehend auch „Union“ oder „EU“ genannt,

und

Neuseeland,

zusammen nachstehend „Vertragsparteien“ genannt,

in Erwägung nachstehender Gründe:

(1) Durch dieses Abkommen, das den Austausch personenbezogener Daten zwischen Europol und den zuständigen neuseeländischen Behörden ermöglicht, wird der Rahmen für eine verstärkte operative Zusammenarbeit zwischen der Europäischen Union und Neuseeland auf dem Gebiet der Strafverfolgung geschaffen, wobei die Menschenrechte und Grundfreiheiten aller betroffenen Personen, einschließlich der Privatsphäre und des Datenschutzes, gewahrt werden.

(2) Dieses Abkommen lässt die Rechtshilfevereinbarungen zwischen Neuseeland und den Mitgliedstaaten der Union, mit denen der Austausch personenbezogener Daten ermöglicht wird, unberührt.

(3) Dieses Abkommen verpflichtet die zuständigen Behörden nicht zur Übermittlung personenbezogener Daten. Der Austausch von personenbezogenen Daten, die im Rahmen dieser Vereinbarung angefordert werden, erfolgt freiwillig.

(4) In dem Abkommen wird anerkannt, dass die Parteien vergleichbare Grundsätze der Verhältnismäßigkeit und Angemessenheit anwenden. Der gemeinsame Wesensgehalt dieser Grundsätze ist das Erfordernis, ein Gleichgewicht zwischen allen betroffenen öffentlichen oder privaten Interessen unter Berücksichtigung aller Umstände des jeweiligen Sachverhalts zu erreichen. Bei einem solchen Gleichgewicht geht es einerseits um das Recht des Einzelnen auf Privatsphäre in Verbindung mit anderen Menschenrechten und Interessen und zum anderen um die gegenläufigen berechtigten Ziele, die verfolgt werden können, wie in diesem Abkommen genannte Zwecke der Verarbeitung personenbezogener Daten —

sind wie folgt übereingekommen:

KAPITEL I – ALLGEMEINE BESTIMMUNGEN

Artikel 1
Gegenstand

In diesem Abkommen ist vorgesehen, die Übermittlung personenbezogener Daten zwischen der Agentur der Europäischen Union für die Zusammenarbeit auf dem Gebiet der Strafverfolgung (Europol) und den zuständigen neuseeländischen Behörden zu ermöglichen, um die Maßnahmen der Behörden der Mitgliedstaaten der Europäischen Union und der neuseeländischen Behörden sowie ihre gegenseitige Zusammenarbeit bei der Verhütung und Bekämpfung von Straftaten, einschließlich schwerer Kriminalität und Terrorismus, zu unterstützen und zu verstärken und gleichzeitig geeignete Garantien in Bezug auf die Menschenrechte und Grundfreiheiten des Einzelnen, einschließlich des Schutzes der Privatsphäre und des Datenschutzes, zu gewährleisten.

Artikel 2
Begriffsbestimmungen

Für die Zwecke dieses Abkommens bezeichnet der Begriff

a) „Vertragsparteien“ die Europäische Union einerseits und Neuseeland andererseits;

b) „Europol“ die Agentur der Europäischen Union für die Zusammenarbeit auf dem Gebiet der Strafverfolgung, die mit der Verordnung (EU) 2016/794[1] oder deren Änderungen eingerichtet wurde (im Folgenden „Europol-Verordnung“);

c) „zuständige Behörde“ im Falle Neuseelands die inländischen Strafverfolgungsbehörden, die nach neuseeländischem Recht für die Verhütung und Bekämpfung der in Anhang II dieses Abkommens aufgeführten Straftaten zuständig sind (im Folgenden „zuständige neuseeländische Behörden“), und im Falle der Europäischen Union Europol;

d) „Unionseinrichtungen“ die Organe, Einrichtungen, Missionen, Ämter und Agenturen, die durch den Vertrag über die Europäische Union und den Vertrag über die Arbeitsweise der Europäischen Union oder auf der Grundlage dieser Verträge geschaffen wurden und in Anhang III aufgeführt sind;

e) „Straftaten“ die in Anhang I aufgeführten Formen der Kriminalität und damit zusammenhängende Straftaten. Straftaten gelten als mit den in Anhang I aufgeführten Formen der Kriminalität in Zusammenhang stehend, wenn sie begangen werden, um die Mittel zur Begehung dieser Formen der Kriminalität zu beschaffen, um solche Formen der Kriminalität zu erleichtern oder durchzuführen oder um dafür zu sorgen, dass sie straflos bleiben;

f) „personenbezogene Daten“ alle Informationen, die sich auf eine betroffene Person beziehen;

[1] Die Verordnung (EU) 2016/794 ist die Verordnung (EU) 2016/794 des Europäischen Parlaments und des Rates vom 11. Mai 2016 über die Agentur der Europäischen Union für die Zusammenarbeit auf dem Gebiet der Strafverfolgung (Europol) und zur Ersetzung und Aufhebung der Beschlüsse 2009/371/JI, 2009/934/JI, 2009/935/JI, 2009/936/JI und 2009/968/JI des Rates (ABl. L 135 vom 24.5.2016, S. 53).

g) „betroffene Person“ eine bestimmte oder bestimmbare natürliche Person; eine bestimmbare Person ist eine Person, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, einer Kennnummer, Standortdaten, einer Online-Kennung oder einem oder mehreren besonderen Merkmalen bestimmt werden kann, die Ausdruck ihrer physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind;

h) „genetische Daten” alle personenbezogenen Daten zu den ererbten oder erworbenen genetischen Merkmalen eines Menschen, die eindeutige Informationen über die Physiologie oder die Gesundheit dieses Menschen liefern und insbesondere aus der Analyse einer biologischen Probe des betreffenden Menschen gewonnen wurden;

i) „Verarbeitung“ jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Weitergabe durch Übermittlung, die Verbreitung oder jede andere Form der Bereitstellung, der Abgleich oder die Verknüpfung, das Löschen oder Vernichten der Daten sowie die Beschränkung des Zugriffs auf Daten;

j) „Information“ personenbezogene Daten;

k) „Verletzung des Schutzes personenbezogener Daten“ eine Verletzung der Sicherheit, die zur Vernichtung, zum Verlust oder zur Veränderung, ob unbeabsichtigt oder widerrechtlich, oder zur unbefugten Weitergabe von beziehungsweise zum unbefugten Zugriff auf personenbezogene Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden;

l) „Kontrollbehörde“ eine oder mehrere inländische unabhängige Behörden, die allein oder kumulativ für den Datenschutz im Sinne von Artikel 16 dieses Abkommens zuständig sind und die gemäß diesem Artikel notifiziert wurden. Dies kann Behörden einschließen, deren Zuständigkeit sich auch auf andere Menschenrechte erstreckt;

m) „internationale Organisation“ eine völkerrechtliche Organisation und ihre nachgeordneten Stellen oder jede sonstige Einrichtung, die durch eine zwischen zwei oder mehr Ländern geschlossene Übereinkunft oder auf der Grundlage einer solchen Übereinkunft geschaffen wurde.

Artikel 3
Zwecke der Verarbeitung personenbezogener Daten

(1) Die im Rahmen des Abkommens angeforderten und empfangenen personenbezogenen Daten werden nur zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung innerhalb der Grenzen von Artikel 4 Absatz 5 und der jeweiligen Mandate der zuständigen Behörden verarbeitet.

(2) Die zuständigen Behörden machen spätestens bei der Übermittlung personenbezogener Daten eindeutige Angaben zu dem spezifischen Zweck oder den spezifischen Zwecken der Übermittlung der Daten. Bei Übermittlungen an Europol müssen der Zweck oder die Zwecke dieser Übermittlungen in Übereinstimmung mit

den im Mandat von Europol festgelegten spezifischen Verarbeitungszwecken festgelegt werden.

KAPITEL II – INFORMATIONSAUSTAUSCH UND DATENSCHUTZ

Artikel 4
Allgemeine Datenschutzgrundsätze

(1) Jede Vertragspartei sorgt dafür, dass die im Rahmen dieses Abkommens ausgetauschten personenbezogenen Daten

a) nach Treu und Glauben, auf rechtmäßiger Grundlage und nur zu dem Zweck verarbeitet werden, zu dem sie gemäß Artikel 3 übermittelt wurden,

b) dem Zweck angemessen und sachlich relevant sowie auf das für die Zwecke der Datenverarbeitung notwendige Maß beschränkt sind,

c) sachlich richtig und auf dem neuesten Stand sind; jede Vertragspartei sieht vor, dass ihre zuständigen Behörden alle angemessenen Maßnahmen treffen, um sicherzustellen, dass personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unzutreffend sind, unverzüglich gelöscht oder berichtigt werden,

d) in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie dies für die Zwecke, für die die personenbezogenen Daten verarbeitet werden, erforderlich ist,

e) auf eine Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten sicherstellt.

(2) Die übermittelnde zuständige Behörde kann bei der Übermittlung personenbezogener Daten etwaige allgemeine oder spezifische Einschränkungen des Zugriffs auf diese Daten oder ihrer Verwendung angeben, einschließlich bezüglich ihrer Weiterübermittlung, Löschung oder Vernichtung nach einer bestimmten Frist sowie der weiteren Verarbeitung. Ergibt sich die Notwendigkeit solcher Einschränkungen nach Bereitstellung der Informationen, so informiert die übermittelnde zuständige Behörde die empfangende Behörde entsprechend.

(3) Jede Vertragspartei stellt sicher, dass die empfangende zuständige Behörde jede von der übermittelnden zuständigen Behörde angegebene Einschränkung des Zugriffs auf oder der Weiterverwendung der personenbezogenen Daten gemäß Absatz 2 beachtet.

(4) Jede Vertragspartei stellt sicher, dass ihre zuständigen Behörden geeignete technische und organisatorische Vorkehrungen treffen, um nachweisen zu können, dass die Datenverarbeitung im Einklang mit diesem Abkommen erfolgt und die Rechte der betroffenen Personen geschützt werden.

(5) Jede Vertragspartei stellt sicher, dass ihre zuständigen Behörden keine personenbezogenen Daten übermitteln, die unter offenkundiger Verletzung der durch die für die Vertragsparteien verbindlichen Normen des Völkerrechts anerkannten Menschenrechte erlangt wurden. Jede Vertragspartei stellt sicher, dass die empfangenen personenbezogenen Daten nicht dazu verwendet werden, um die

Todesstrafe oder eine Form der grausamen und unmenschlichen Behandlung zu beantragen, zu verhängen oder zu vollstrecken.

(6) Jede Vertragspartei stellt sicher, dass alle Übermittlungen personenbezogener Daten im Rahmen dieses Abkommens sowie der Zweck oder die Zwecke dieser Übermittlungen dokumentiert werden.

Artikel 5
Besondere Kategorien personenbezogener Daten und verschiedene Kategorien von betroffenen Personen

(1) Die Übermittlung personenbezogener Daten in Bezug auf Opfer von Straftaten, Zeugen oder andere Personen, die Informationen über Straftaten liefern können, oder in Bezug auf Personen unter 18 Jahren ist verboten, es sei denn, die Übermittlung ist im Einzelfall für die Verhütung oder Bekämpfung einer Straftat unbedingt erforderlich sowie angemessen und verhältnismäßig.

(2) Die Übermittlung personenbezogener Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Übermittlung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person oder von Gesundheitsdaten oder Daten zum Sexualleben oder zu der sexuellen Ausrichtung einer natürlichen Person ist nur zulässig, wenn dies für die Verhütung oder Bekämpfung einer Straftat unbedingt erforderlich sowie im Einzelfall angemessen und verhältnismäßig ist und wenn diese Daten, mit Ausnahme biometrischer Daten, andere personenbezogene Daten ergänzen.

(3) Die Vertragsparteien stellen sicher, dass die Verarbeitung personenbezogener Daten nach den Absätzen 1 und 2 geeigneten Garantien unterliegt, die sich auf die damit verbundenen besonderen Risiken erstrecken, einschließlich Einschränkungen des Zugriffs, zusätzlicher Sicherheitsmaßnahmen im Sinne von Artikel 15 und Beschränkungen der Weiterübermittlung nach Artikel 7.

Artikel 6
Automatisierte Verarbeitung personenbezogener Daten

Entscheidungen, die ausschließlich auf einer automatisierten Verarbeitung der ausgetauschten personenbezogenen Daten beruhen, einschließlich Profiling, ohne menschliches Eingreifen, die nachteilige rechtliche Folgen für eine betroffene Person nach sich ziehen oder sie erheblich beeinträchtigen können, sind untersagt, es sei denn, sie sind zur Verhütung oder Bekämpfung einer Straftat gesetzlich zulässig und es bestehen angemessene Garantien für die Rechte und Freiheiten der betroffenen Person, einschließlich wenigstens des Rechts auf Erwirkung des menschlichen Eingreifens.

Artikel 7
Weiterübermittlung der empfangenen personenbezogenen Daten

(1) Neuseeland stellt sicher, dass seine zuständigen Behörden personenbezogene Daten, die sie im Rahmen dieses Abkommens empfangen haben, nur an andere Behörden in Neuseeland weiterübermitteln, wenn

a) Europol ihre vorherige ausdrückliche Genehmigung erteilt hat,

b) der Zweck der Weiterübermittlung derselbe ist wie der ursprüngliche Zweck der Übermittlung durch Europol oder innerhalb der Grenzen von Artikel 3 Absatz 1 in direktem Zusammenhang mit diesem ursprünglichen Zweck steht und

c) für die Weiterübermittlung dieselben Bestimmungen und Garantien wie für die ursprüngliche Übermittlung gelten.

(2) Unbeschadet des Artikels 4 Absatz 2 ist keine vorherige Genehmigung erforderlich, wenn die empfangende Behörde selbst eine zuständige Behörde Neuseelands ist. Gleiches gilt für die Möglichkeit von Europol, personenbezogene Daten an die in den Mitgliedstaaten der Europäischen Union für die Verhütung und Bekämpfung von Straftaten zuständigen Behörden und die in Anhang III aufgeführten Einrichtungen der Union weiter zu übermitteln.

(3) Neuseeland stellt sicher, dass die Weiterübermittlung von personenbezogenen Daten, die seine zuständigen Behörden im Rahmen dieses Abkommens empfangen haben, an die Behörden eines Drittstaats oder an eine internationale Organisation untersagt ist, es sei denn, die folgenden Bedingungen sind erfüllt:

a) Die Übermittlung betrifft andere personenbezogene Daten als diejenigen, die unter Artikel 5 des Abkommens fallen,

b) Europol ihre vorherige ausdrückliche Genehmigung erteilt hat,

c) der Zweck der Weiterübermittlung ist derselbe wie der ursprüngliche Zweck der Übermittlung durch Europol, und

d) für die Weiterübermittlung gelten dieselben Bestimmungen und Garantien wie für die ursprüngliche Übermittlung.

(4) Europol kann ihre Genehmigung nach Absatz 3 Buchstabe b für eine Weiterübermittlung an die Behörde eines Drittstaats oder an eine internationale Organisation nur erteilen, wenn oder insoweit ein Angemessenheitsbeschluss, eine internationale Übereinkunft, die angemessene Garantien hinsichtlich des Schutzes der Privatsphäre, der Grundrechte und der Freiheiten von natürlichen Personen bietet, ein Kooperationsabkommen oder eine andere künftige Rechtsgrundlage für die Übermittlung personenbezogener Daten im Sinne der Europol-Verordnung, die die Weiterübermittlung abdeckt, vorliegt.

(5) Die Europäische Union stellt sicher, dass die Weiterübermittlung von personenbezogenen Daten, die Europol im Rahmen dieses Abkommens empfangen hat, an nicht in Anhang III aufgeführte Einrichtungen der Europäischen Union, Behörden von Drittstaaten oder internationale Organisationen untersagt ist, es sei denn,

a) die Übermittlung betrifft andere personenbezogene Daten als diejenigen, die unter Artikel 5 des Abkommens fallen,

b) Neuseeland hat seine vorherige ausdrückliche Genehmigung erteilt,

c) der Zweck der Weiterübermittlung ist derselbe wie der ursprüngliche Zweck der Übermittlung durch Neuseeland, und

d) es liegt ein Angemessenheitsbeschluss, eine internationale Übereinkunft, die angemessene Garantien hinsichtlich des Schutzes der Privatsphäre, der Grundrechte und der Freiheiten von natürlichen Personen bietet, oder ein Kooperationsabkommen im Sinne der Europol-Verordnung mit dem betreffenden Drittstaat oder der betreffenden internationalen Organisation vor.

Artikel 8
Bewertung der Zuverlässigkeit der Quelle und Richtigkeit der Informationen

(1) Die Zuverlässigkeit der Quelle wird von den zuständigen Behörden nach Möglichkeit spätestens bei der Übermittlung der Informationen anhand eines oder mehrerer der folgenden Kriterien angegeben:

1. Es bestehen keine Zweifel an der Authentizität, Verlässlichkeit und Eignung der Quelle, oder die Informationen stammen von einer Quelle, die sich in der Vergangenheit in allen Fällen als verlässlich erwiesen hat;

2. die Informationen stammen von einer Quelle, deren Informationen sich in den meisten Fällen als verlässlich erwiesen haben;

3. die Informationen stammen von einer Quelle, deren Informationen sich in den meisten Fällen als nicht verlässlich erwiesen haben;

4. die Verlässlichkeit der Quelle kann nicht beurteilt werden.

(2) Die Richtigkeit der Informationen wird von den zuständigen Behörden nach Möglichkeit spätestens bei der Übermittlung der Informationen anhand eines oder mehrerer der folgenden Kriterien angegeben:

1. Informationen, deren Richtigkeit zum Zeitpunkt der Übermittlung nicht angezweifelt wird;

2. Informationen, die der Quelle, nicht aber dem Beamten, der sie weitergibt, persönlich bekannt sind;

3. Informationen, die der Quelle nicht persönlich bekannt sind, die aber durch andere bereits erfasste Informationen erhärtet werden;

4. Informationen, die der Quelle nicht persönlich bekannt sind und die sich auf keine andere Weise erhärten lassen.

(3) Kommt die empfangende zuständige Behörde auf der Grundlage bereits in ihrem Besitz befindlicher Informationen zu dem Schluss, dass die von der übermittelnden zuständigen Behörde gemäß den Absätzen 1 und 2 bereitgestellte Beurteilung der Informationen oder ihrer Quelle berichtigt werden muss, setzt sie diese Behörde darüber in Kenntnis und versucht, sich auf eine Änderung der Beurteilung zu einigen. Ohne dieses Einvernehmen darf die empfangende zuständige Behörde die Beurteilung der erhaltenen Informationen oder der Quelle der Informationen nicht ändern.

(4) Wenn eine zuständige Behörde Informationen ohne Beurteilung erhält, versucht sie, soweit und wo es möglich ist, im Einvernehmen mit der übermittelnden zuständigen Behörde die Zuverlässigkeit der Quelle oder die Richtigkeit der Informationen auf der Grundlage bereits in ihrem Besitz befindlicher Informationen zu beurteilen.

(5) Kann keine zuverlässige Beurteilung vorgenommen werden, sind die Informationen nach Absatz 1 Ziffer 4 und Absatz 2 Ziffer 4 zu beurteilen.

RECHTE DER BETROFFENEN PERSON

Artikel 9
Recht auf Auskunft

(1) Die Vertragsparteien stellen sicher, dass die betroffene Person das Recht hat, in angemessenen Abständen Auskunft darüber zu erhalten, ob sie betreffende personenbezogene Daten im Rahmen dieses Abkommens verarbeitet werden; ist dies der Fall, erhält die betroffene Person mindestens Folgendes:

a) eine Bestätigung, ob sie betreffende Daten verarbeitet wurden oder nicht,

b) zumindest Angaben zu den Zwecken der Verarbeitung, den Datenkategorien, die verarbeitet werden, und gegebenenfalls den Empfängern oder Kategorien von Empfängern, an die die Daten übermittelt werden,

c) das Bestehen eines Rechts auf Berichtigung oder Löschung personenbezogener Daten oder auf Einschränkung der Verarbeitung der personenbezogenen Daten der betroffenen Person durch die zuständige Behörde,

d) eine Angabe der Rechtsgrundlage für die Datenverarbeitung,

e) falls möglich, die vorgesehene Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer,

f) eine Mitteilung in verständlicher Form über die personenbezogenen Daten, die Gegenstand der Verarbeitung sind, sowie über alle verfügbaren Informationen zur Herkunft der Daten.

(2) In Fällen, in denen das Recht auf Auskunft ausgeübt wird, ist die übermittelnde Vertragspartei unverbindlich zu konsultieren, bevor eine endgültige Entscheidung über den Antrag getroffen wird.

(3) Die Vertragsparteien können vorsehen, dass die Bereitstellung von Informationen auf einen Antrag nach Absatz 1 verzögert, verweigert oder eingeschränkt werden kann, sofern und solange eine solche Verzögerung, Verweigerung oder Einschränkung eine Maßnahme darstellt, die unter Berücksichtigung der Grundrechte und Interessen der betroffenen Personen erforderlich sowie angemessen und verhältnismäßig ist, um

a) sicherzustellen, dass strafrechtliche Ermittlungen und die Strafverfolgung nicht gefährdet werden, oder

b) die Rechte und Freiheiten Dritter zu schützen oder

c) die Sicherheit und die öffentliche Ordnung zu schützen oder Straftaten zu verhüten.

(4) Die Vertragsparteien stellen sicher, dass die zuständige Behörde die betroffene Person schriftlich über jede Verzögerung, Verweigerung oder Einschränkung des Rechts auf Auskunft und über die Gründe dafür unterrichtet. Diese Gründe können entfallen, sofern und solange dies den Zweck der Verzögerung, Verweigerung oder Einschränkung nach Absatz 3 untergraben würde. Die zuständige Behörde unterrichtet die betroffene Person über die Möglichkeit, eine Beschwerde bei den jeweiligen Kontrollbehörden einzureichen, sowie über andere Rechtsbehelfe, die in ihrem jeweiligen Rechtsrahmen vorgesehen sind.

Artikel 10
Recht auf Berichtigung, Löschung und Einschränkung

(1) Die Vertragsparteien stellen sicher, dass die betroffene Person das Recht hat, die zuständigen Behörden aufzufordern, unrichtige personenbezogene Daten über die betroffene Person, die im Rahmen des Abkommens übermittelt wurden, zu berichtigen. Unter Berücksichtigung der Zwecke der Verarbeitung schließt dies das Recht ein, dass unvollständige personenbezogener Daten, die im Rahmen des Abkommens übermittelt werden, vervollständigt werden.

(2) Die Berichtigung schließt die Löschung von personenbezogenen Daten ein, die für den Zweck bzw. die Zwecke, für den bzw. die sie verarbeitet werden, nicht mehr erforderlich sind.

(3) Die Vertragsparteien können anstelle der Löschung personenbezogener Daten gemäß Absatz 2 die Einschränkung der Verarbeitung vorsehen, wenn berechtigter Grund zu der Annahme besteht, dass die Löschung die schutzwürdigen Interessen der betroffenen Personen beeinträchtigen würde.

(4) Die zuständigen Behörden unterrichten sich gegenseitig über die gemäß den Absätzen 1, 2 und 3 getroffenen Maßnahmen. Die empfangende zuständige Behörde berichtigt, löscht oder schränkt die Verarbeitung solcher Daten im Einklang mit den Maßnahmen der übermittelnden zuständigen Behörde ein.

(5) Die Vertragsparteien sehen vor, dass die zuständige Behörde, bei der der Antrag eingegangen ist, der betroffenen Person binnen kürzester Frist, spätestens aber innerhalb von drei Monaten nach Eingang eines Antrags nach Absatz 1 oder 2, schriftlich mitteilt, dass die die betroffene Person betreffenden Daten berichtigt oder gelöscht würden bzw. ihre Verarbeitung eingeschränkt wurde.

(6) Die Vertragsparteien stellen sicher, dass die zuständige Behörde, bei der der Antrag eingegangen ist, der betroffenen Person binnen kürzester Frist, spätestens aber innerhalb von drei Monaten nach Eingang eines Antrags, schriftlich mitteilt, ob die Berichtigung, Löschung oder die Einschränkung der Verarbeitung verweigert wird, welche Gründe für die Verweigerung vorliegen, dass die Möglichkeit besteht, bei den jeweiligen Kontrollbehörden eine Beschwerde einzureichen, und dass andere Rechtsbehelfe zur Verfügung stehen, die in ihrem jeweiligen Rechtsrahmen vorgesehen sind.

Artikel 11
Meldung von Verletzungen des Schutzes personenbezogener Daten an die betreffenden Behörden

(1) Die Vertragsparteien stellen sicher, dass im Falle einer Verletzung des Schutzes personenbezogener Daten, die sich auf die im Rahmen dieses Abkommens übermittelten personenbezogenen Daten auswirkt, die jeweils zuständigen Behörden einander sowie ihren jeweiligen Kontrollbehörden die Verletzung des Schutzes personenbezogener Daten unverzüglich melden und Maßnahmen ergreifen, um die möglichen nachteiligen Folgen zu begrenzen.

(2) Die Meldung enthält mindestens folgende Angaben:

a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, wenn möglich, unter Angabe der Kategorien und der Zahl der betroffenen Personen sowie der betroffenen Kategorien und der Zahl der betroffenen personenbezogenen Datensätze,

b) eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten,

c) eine Beschreibung der von der zuständigen Behörde getroffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und der ergriffenen Maßnahmen zur Begrenzung ihrer möglichen nachteiligen Folgen.

(3) Sofern es nicht möglich ist, alle erforderlichen Informationen gleichzeitig bereitzustellen, können diese schrittweise bereitgestellt werden. Noch zu liefernde Informationen werden unverzüglich bereitgestellt.

(4) Die Vertragsparteien stellen sicher, dass ihre jeweils zuständigen Behörden alle Verletzungen des Schutzes personenbezogener Daten erfassen, die sich auf die im Rahmen dieses Abkommens übermittelten personenbezogenen Daten auswirken, einschließlich der Fakten im Zusammenhang mit der Verletzung, ihrer Auswirkungen und der ergriffenen Abhilfemaßnahmen, damit ihre jeweilige Kontrollbehörde die Erfüllung ihrer jeweiligen rechtlichen Verpflichtungen überprüfen kann.

Artikel 12
Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person

(1) Die Vertragsparteien sehen für den Fall, dass eine Verletzung des Schutzes personenbezogener Daten im Sinne des Artikels 11 wahrscheinlich ernsthafte nachteilige Auswirkungen auf die Rechte und Freiheiten der betroffenen Person hat, vor, dass ihre jeweils zuständigen Behörden die betroffene Person unverzüglich von der Verletzung des Schutzes personenbezogener Daten benachrichtigen.

(2) Die Benachrichtigung der betroffenen Person nach Absatz 1 umfasst soweit möglich eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, eine Angabe empfohlener Maßnahmen zur Eindämmung etwaiger nachteiliger Auswirkungen der Verletzung des Schutzes personenbezogener Daten sowie die

Angabe des Namen und der Kontaktdaten der Kontaktstelle, bei der weitere Informationen eingeholt werden können.

(3) Die in Absatz 1 genannte Benachrichtigung der betroffenen Person ist nicht erforderlich, wenn

a) die personenbezogenen Daten, die von der Verletzung betroffen sind, Gegenstand geeigneter technischer Schutzmaßnahmen waren, die die betreffenden Daten für alle Personen, die nicht zum Zugriff befugt sind, verschlüsseln,

b) nachfolgende Maßnahmen ergriffen wurden, um sicherzustellen, dass die Rechte und Freiheiten der betroffenen Personen aller Wahrscheinlichkeit nach nicht mehr erheblich beeinträchtigt werden, oder

c) die Benachrichtigung insbesondere angesichts der Zahl der betroffenen Fälle mit einem unverhältnismäßigen Aufwand verbunden wäre. In diesem Fall werden die betroffenen Personen stattdessen durch eine öffentliche Bekanntmachung oder auf ähnlich wirksame Weise informiert.

(4) Die Benachrichtigung der betroffenen Person kann verzögert, eingeschränkt oder unterlassen werden, wenn eine solche Benachrichtigung wahrscheinlich dazu führen würde, dass

a) behördliche oder gerichtliche Untersuchungen, Ermittlungen oder Verfahren behindert werden,

b) die Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder die Vollstreckung von strafrechtlichen Sanktionen, die öffentliche Ordnung oder die nationale Sicherheit beeinträchtigt wird,

c) Auswirkungen auf die Rechte und Freiheiten Dritter entstehen,

sofern dies – unter gebührender Berücksichtigung der schutzwürdigen Interessen der betroffenen Personen – eine erforderliche sowie angemessene und verhältnismäßige Maßnahme darstellt.

Artikel 13
Speicherung, Überprüfung, Berichtigung und Löschung personenbezogener Daten

(1) Die Vertragsparteien sehen angemessene Fristen für die Speicherung der im Rahmen dieses Abkommens empfangenen personenbezogenen Daten oder eine regelmäßige Überprüfung der Notwendigkeit der Speicherung dieser Daten vor, sodass die Daten nur so lange gespeichert werden, wie dies für den Zweck, für den sie übermittelt werden, erforderlich ist.

(2) In jedem Fall wird die Notwendigkeit der weiteren Speicherung spätestens drei Jahre nach Übermittlung der personenbezogenen Daten überprüft, und wird keine begründete und dokumentierte Fortsetzung der Speicherung beschlossen, werden diese Daten nach drei Jahren automatisch gelöscht.

(3) Hat eine zuständige Behörde Grund zu der Annahme, dass zuvor von ihr übermittelte personenbezogene Daten unrichtig oder unzutreffend sind, nicht mehr auf dem neuesten Stand sind oder nicht hätten übermittelt werden dürfen, so unterrichtet sie die empfangende zuständige Behörde, die die personenbezogenen Daten berichtigt oder löscht und die übermittelnde Behörde davon in Kenntnis setzt.

(4) Hat eine zuständige Behörde Grund zu der Annahme, dass zuvor von ihr empfangene personenbezogene Daten unrichtig oder unzutreffend sind, nicht mehr auf dem neuesten Stand sind oder nicht hätten übermittelt werden dürfen, so unterrichtet sie die übermittelnde zuständige Behörde, die dazu Stellung nimmt. Gelangt die übermittelnde zuständige Behörde zu dem Schluss, dass die personenbezogenen Daten unrichtig oder unzutreffend sind, nicht mehr auf dem neuesten Stand sind oder nicht hätten übermittelt werden dürfen, so unterrichtet sie die empfangende zuständige Behörde, die die personenbezogenen Daten berichtigt oder löscht und die übermittelnde Behörde davon in Kenntnis setzt.

Artikel 14
Protokollierung und Dokumentierung

Die Vertragsparteien sorgen für die Protokollierung der Erhebung, der Änderung, des Zugriffs auf, der Offenlegung einschließlich der Weiterübermittlung, der Verknüpfung und der Löschung personenbezogener Daten.

Diese Protokolle oder Dokumentationen werden der zuständigen Kontrollbehörde auf Ersuchen für die Zwecke der Überwachung der Rechtmäßigkeit der Datenverarbeitung, der Selbstüberwachung und der Gewährleistung einer angemessenen Datenintegrität und Sicherheit der Datenverarbeitung zur Verfügung gestellt.

Artikel 15
Datensicherheit

Die Vertragsparteien sorgen für die Umsetzung technischer und organisatorischer Vorkehrungen zum Schutz der im Rahmen dieses Abkommens ausgetauschten personenbezogenen Daten.

In Bezug auf die automatisierte Datenverarbeitung sorgen die Vertragsparteien für die Umsetzung von Maßnahmen, die geeignet sind,

a) Unbefugten den Zugang zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren (Zugangskontrolle),

b) zu verhindern, dass Datenträger unbefugt gelesen, kopiert, verändert oder entfernt werden (Datenträgerkontrolle),

c) die unbefugte Eingabe von personenbezogenen Daten sowie die unbefugte Kenntnisnahme, Änderung oder Löschung von gespeicherten personenbezogenen Daten zu verhindern (Speicherkontrolle),

d) zu verhindern, dass automatisierte Datenverarbeitungssysteme mithilfe von Einrichtungen zur Datenübertragung von Unbefugten genutzt werden können (Benutzerkontrolle),

e) zu gewährleisten, dass die zur Benutzung eines automatisierten Datenverarbeitungssystems Berechtigten nur auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können (Zugriffskontrolle),

f) zu gewährleisten, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten durch Einrichtungen zur Datenübertragung übermittelt werden können oder übermittelt worden sind (Übermittlungskontrolle),

g) zu gewährleisten, dass überprüft und festgestellt werden kann, welche personenbezogenen Daten wann und von wem in automatisierte Datenverarbeitungssysteme eingegeben worden sind (Eingabekontrolle),

h) zu gewährleisten, dass überprüft und festgestellt werden kann, auf welche Daten von welchem Mitarbeiter zu welcher Zeit zugegriffen wurde (Zugriffsprotokoll),

i) zu verhindern, dass bei der Übertragung personenbezogener Daten sowie beim Transport von Datenträgern die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können (Transportkontrolle),

j) zu gewährleisten, dass eingesetzte Systeme im Störungsfall unverzüglich wiederhergestellt werden können (Wiederherstellung),

k) zu gewährleisten, dass die Funktionen des Systems fehlerfrei ablaufen, auftretende Fehlfunktionen unverzüglich gemeldet werden (Verlässlichkeit) und gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems verfälscht werden (Unverfälschtheit).

Artikel 16
Kontrollbehörde

(1) Jede Vertragspartei stellt sicher, dass es eine unabhängige öffentliche Behörde gibt, die für den Datenschutz zuständig ist (Kontrollbehörde), um Angelegenheiten zu überwachen, die die Privatsphäre des Einzelnen betreffen, einschließlich der innerstaatlichen Vorschriften, die im Rahmen dieses Abkommens für den Schutz der Grundrechte und der Freiheiten natürlicher Personen in Bezug auf die Verarbeitung personenbezogener Daten von Bedeutung sind. Die Vertragsparteien teilen einander die Behörde mit, die sie als Kontrollbehörde im Sinne dieses Artikels bezeichnen.

(2) Die Vertragsparteien stellen sicher, dass die Kontrollbehörde bei der Erfüllung ihrer Aufgaben und der Ausübung ihrer Befugnisse völlig unabhängig handelt. Sie handelt frei von äußerer Beeinflussung und fordert weder Weisungen an noch nimmt sie Weisungen entgegen. Ihre Mitglieder verfügen über eine gesicherte Amtszeit, einschließlich Schutzmaßnahmen gegen willkürliche Amtsenthebung.

(3) Die Vertragsparteien stellen sicher, dass jede Kontrollbehörde über die personellen, technischen und finanziellen Mittel, die Räumlichkeiten und die Infrastrukturen verfügt, die für die wirksame Erfüllung ihrer Aufgaben und die Ausübung ihrer Befugnisse erforderlich sind.

(4) Die Vertragsparteien stellen sicher, dass jede Kontrollbehörde mit wirksamen Untersuchungs- und Eingriffsbefugnissen ausgestattet ist, um die Aufsicht über die von ihr beaufsichtigten Stellen ausüben und Gerichtsverfahren anstrengen zu können.

(5) Die Vertragsparteien stellen sicher, dass jede Kontrollbehörde befugt ist, Beschwerden von Einzelpersonen über die Verwendung ihrer personenbezogenen Daten durch die ihrer Überwachung unterliegenden zuständigen Behörden entgegenzunehmen.

Artikel 17
Verwaltungsrechtlicher und gerichtlicher Rechtsbehelf

Die betroffenen Personen haben das Recht auf einen wirksamen verwaltungsrechtlichen und gerichtlichen Rechtsbehelf, wenn die in diesem Abkommen anerkannten Rechte und Garantien infolge der Verarbeitung ihrer personenbezogenen Daten verletzt wurden. Die Vertragsparteien teilen einander die innerstaatlichen Rechtsvorschriften mit, die nach ihrer Auffassung die in diesem Artikel garantierten Rechte gewährleisten.

KAPITEL III – STREITIGKEITEN

Artikel 18
Streitbeilegung

Alle Streitigkeiten, die im Zusammenhang mit der Auslegung, Anwendung oder Durchführung dieses Abkommens und damit zusammenhängenden Fragen auftreten können, sind Gegenstand von Konsultationen und Verhandlungen zwischen Vertretern der Vertragsparteien, mit dem Ziel, eine einvernehmliche Lösung zu finden.

Artikel 19
Aussetzungsklausel

(1) Im Falle einer schwerwiegenden Verletzung oder Nichterfüllung der sich aus den Bestimmungen dieses Abkommens ergebenden Pflichten kann jede Vertragspartei dieses Abkommen durch schriftliche Notifikation an die andere Vertragspartei auf diplomatischem Wege vorübergehend ganz oder teilweise aussetzen. Eine solche schriftliche Notifikation kann erst erfolgen, wenn die Vertragsparteien einander während eines angemessenen Zeitraums konsultiert, jedoch dabei keine Lösung gefunden haben; die Aussetzung tritt nach einer Frist von zwanzig Tagen ab dem Tag des Eingangs dieser Notifikation in Kraft. Eine solche Aussetzung kann von der aussetzenden Vertragspartei durch schriftliche Notifikation an die andere Vertragspartei aufgehoben werden. Die Aufhebung wird unmittelbar nach Eingang einer solchen Notifikation wirksam.

(2) Ungeachtet einer etwaigen Aussetzung dieses Abkommens werden personenbezogene Daten, die in den Anwendungsbereich dieses Abkommens fallen und vor der Aussetzung übermittelt wurden, weiterhin gemäß den Bestimmungen dieses Abkommens verarbeitet.

Artikel 20
Kündigung des Abkommens

(1) Dieses Abkommen kann von jeder der Vertragsparteien jederzeit durch schriftliche Notifizierung auf diplomatischem Wege unter Einhaltung einer Frist von drei Monaten gekündigt werden.

(2) Personenbezogene Daten, die in den Anwendungsbereich dieses Abkommens fallen und vor deren Kündigung übermittelt wurden, werden zum Zeitpunkt der Kündigung weiterhin gemäß den Bestimmungen dieses Abkommens verarbeitet.

(3) Im Falle einer Kündigung einigen sich die Vertragsparteien auf die weitere Verwendung und Speicherung der Informationen, die bereits zwischen ihnen ausgetauscht wurden.

KAPITEL IV – SCHLUSSBESTIMMUNGEN

Artikel 21
Beziehung zu anderen internationalen Instrumenten

(1) Dieses Abkommen berührt nicht die rechtlichen Bestimmungen über den Informationsaustausch zwischen Neuseeland und einem Mitgliedstaat der Europäischen Union, die in einem Rechtshilfeabkommen, einem anderem Kooperationsabkommen oder einer anderen Vereinbarung oder einer Arbeitsregelung auf dem Gebiet der Strafverfolgung für den Informationsaustausch zwischen Neuseeland und einem Mitgliedstaat der Europäischen Union vorgesehen sind, und wirkt sich auch nicht in anderer Weise darauf aus.

(2) Dieses Abkommen ergänzt die Arbeitsvereinbarung mit dem Titel „Working Arrangement establishing cooperative relations between New Zealand Police and the European Union Agency for Law Enforcement Cooperation“ (Arbeitsvereinbarung zur Aufnahme von Kooperationsbeziehungen zwischen der neuseeländischen Polizei und der Agentur der Europäischen Union für die Zusammenarbeit auf dem Gebiet der Strafverfolgung).

Artikel 22
Verwaltungsrechtliche Durchführungsvereinbarung

Die Einzelheiten der Zusammenarbeit zwischen den Vertragsparteien zur Durchführung dieses Abkommens werden in einer verwaltungsrechtlichen Durchführungsvereinbarung zwischen Europol und den zuständigen neuseeländischen Behörden im Einklang mit der Europol-Verordnung geregelt.

Artikel 23
Verwaltungsvereinbarung über die Vertraulichkeit

Der Austausch von EU-Verschlusssachen, der im Rahmen dieses Abkommens gegebenenfalls erforderlich ist, wird durch eine Verwaltungsvereinbarung über die Vertraulichkeit zwischen Europol und den zuständigen neuseeländischen Behörden geregelt.

Artikel 24
Nationale Kontaktstelle und Verbindungsbeamte

(1) Neuseeland benennt eine nationale Kontaktstelle, die als zentrale Kontaktstelle zwischen Europol und den zuständigen neuseeländischen Behörden fungiert. Die besonderen Aufgaben der nationalen Kontaktstelle werden in der verwaltungsrechtlichen Durchführungsvereinbarung nach Artikel 22 Absatz 1 aufgeführt. Die benannte nationale Kontaktstelle für Neuseeland ist in Anhang IV aufgeführt.

(2) Europol und Neuseeland verstärken ihre Zusammenarbeit nach diesem Abkommen durch die Entsendung eines oder mehrerer neuseeländischer Verbindungsbeamter. Europol kann einen oder mehrere Verbindungsbeamte nach Neuseeland entsenden.

Artikel 25
Kosten

Die Vertragsparteien stellen sicher, dass die zuständigen Behörden ihre im Zuge der Durchführung dieses Abkommens anfallenden Kosten selbst tragen, sofern in diesem Abkommen oder in der Verwaltungsvereinbarung nichts anderes festgelegt ist.

Artikel 26
Notifizierung der Durchführung

(1) Jede Vertragspartei stellt sicher, dass ihre zuständigen Behörden ein Dokument öffentlich zugänglich machen, in dem die Bestimmungen für die Verarbeitung personenbezogener Daten, die im Rahmen dieses Abkommens übermittelt werden, einschließlich der Möglichkeiten der betroffenen Personen zur Ausübung ihrer Rechte, in verständlicher Form dargelegt sind. Jede Vertragspartei stellt sicher, dass der anderen Vertragspartei eine Kopie dieses Dokuments übermittelt wird.

(2) Sofern nicht bereits vorhanden, legen die zuständigen Behörden genaue Regeln fest, wie die Einhaltung der Bestimmungen über die Verarbeitung von personenbezogenen Daten in der Praxis durchgesetzt werden wird. Eine Kopie dieser Regeln wird der anderen Vertragspartei und den jeweiligen Kontrollbehörden übermittelt.

Artikel 27
Inkrafttreten und Gültigkeit

(1) Dieses Abkommen wird von den Vertragsparteien nach ihren eigenen internen Verfahren genehmigt.

(2) Dieses Abkommen tritt an dem Tag in Kraft, an dem die letzte schriftliche Notifikation eingeht, mit der die Vertragsparteien einander auf diplomatischem Wege mitgeteilt haben, dass die in Absatz 1 genannten Verfahren abgeschlossen sind.

(3) Dieses Abkommen tritt am ersten Tag nach dem Tag in Kraft, an dem alle folgenden Bedingungen erfüllt sind:

a) die in Artikel 22 festgelegte verwaltungsrechtliche Durchführungsvereinbarung ist anwendbar geworden und

b) die Vertragsparteien haben einander mitgeteilt, dass die in diesem Abkommen festgelegten Pflichten, einschließlich der in Artikel 26 festgelegten Pflichten, erfüllt wurden, und diese Notifikation wurde angenommen.

(4) Die Vertragsparteien tauschen auf diplomatischem Wege schriftliche Notifikationen, in denen die Erfüllung der oben genannten Bedingungen bestätigt wird, aus.

Artikel 28
Änderungen und Ergänzungen

(1) Dieses Abkommen kann jederzeit im gegenseitigen Einvernehmen der Vertragsparteien durch eine auf diplomatischem Wege ausgetauschte schriftliche Notifikation geändert werden. Die Änderungen treten nach demselben rechtlichen Verfahren in Kraft, das in Artikel 27 Absätze 1 und 2 vorgesehen ist.

(2) Die Anhänge zu diesem Abkommen können bei Bedarf durch einen diplomatischen Notenwechsel aktualisiert werden. Solche Aktualisierungen treten gemäß Artikel 27 Absätze 1 und 2 in Kraft.

(3) Die Vertragsparteien nehmen auf Ersuchen einer der Vertragsparteien Konsultationen über die Änderung dieses Abkommens oder seiner Anhänge auf.

Artikel 29
Überprüfung und Bewertung

(1) Die Vertragsparteien überprüfen gemeinsam ein Jahr nach Inkrafttreten dieses Abkommens und dann in regelmäßigen Abständen und zusätzlich auf Ersuchen einer Vertragspartei und eines gemeinsamen Beschlusses die Durchführung dieses Abkommens.

(2) Die Parteien bewerten das Abkommen gemeinsam vier Jahre nach seinem Inkrafttreten.

(3) Die Vertragsparteien legen die Modalitäten der Überprüfung der Durchführung des Abkommens im Voraus fest und teilen einander die Zusammensetzung ihrer jeweiligen Teams mit. Die Teams setzen sich aus einschlägigen Experten für Datenschutz und Strafverfolgung zusammen. Vorbehaltlich geltender Rechtsvorschriften müssen alle an der Überprüfung teilnehmenden Personen die Vertraulichkeit der Beratungen wahren und einer angemessenen Sicherheitsüberprüfung unterzogen worden sein. Für die Zwecke einer Überprüfung gewährleisten Neuseeland und die Europäische Union den Zugang zu den einschlägigen Dokumentationen, Systemen und Mitarbeitern.

Artikel 30
Räumlicher Anwendungsbereich

(1) Dieses Abkommen gilt für das Gebiet, in dem und insofern der Vertrag über die Europäische Union und der Vertrag über die Arbeitsweise der Europäischen Union angewandt werden, und für das Hoheitsgebiet Neuseelands.

(2) Dieses Abkommen gilt nur dann für das Hoheitsgebiet Dänemarks oder Irlands, wenn die Europäische Union Neuseeland schriftlich notifiziert, dass Dänemark oder Irland beschlossen hat, durch die Bestimmungen des Abkommens gebunden zu sein.

(3) Notifiziert die Europäische Union Neuseeland vor dem Inkrafttreten dieses Abkommens, dass es auf das Hoheitsgebiet Dänemarks oder Irlands Anwendung findet, so gilt dieses Abkommen für das Hoheitsgebiet des betreffenden Mitgliedstaats ab demselben Tag, an dem es für die anderen Mitgliedstaaten der Europäischen Union gilt.

(4) Notifiziert die Europäische Union Neuseeland nach Inkrafttreten dieses Abkommens, dass es auf das Hoheitsgebiet Dänemarks oder Irlands Anwendung findet, so gilt dieses Abkommen für das Hoheitsgebiet des betreffenden Mitgliedstaats 30 Tage nach dem Datum der Notifikation.

Geschehen zu am in jeweils zwei Urschriften in bulgarischer, dänischer, deutscher, englischer, estnischer, finnischer, französischer, griechischer, italienischer, kroatischer, lettischer, litauischer, maltesischer, niederländischer, polnischer, portugiesischer, rumänischer, schwedischer, slowakischer, slowenischer, spanischer, tschechischer und ungarischer Sprache, wobei jeder Wortlaut gleichermaßen verbindlich ist.

Für **Neuseeland** Für **die EU**

ANHANG I – KRIMINALITÄTSBEREICHE

Die folgenden Straftaten sind Straftaten im Sinne von Artikel 2 Buchstabe e:

– Terrorismus,

– organisierte Kriminalität,

– Drogenhandel,

– Geldwäschehandlungen,

– Kriminalität im Zusammenhang mit nuklearen und radioaktiven Substanzen,

– Schleuserkriminalität,

– Menschenhandel,

– Kraftfahrzeugkriminalität,

– Mord, schwere Körperverletzung,

– illegaler Handel mit menschlichen Organen und menschlichem Gewebe,

– Entführung, Freiheitsberaubung und Geiselnahme,

– Rassismus und Fremdenfeindlichkeit,

– Raub und schwerer Diebstahl,

– illegaler Handel mit Kulturgütern, einschließlich Antiquitäten und Kunstgegenständen,

– Betrugsdelikte,

– gegen die finanziellen Interessen der EU gerichtete Straftaten,

– Insidergeschäfte und Finanzmarktmanipulation,

– Erpressung und Schutzgelderpressung,

– Nachahmung und Produktpiraterie,

– Fälschung von amtlichen Dokumenten und Handel damit,

– Geldfälschung, Fälschung von Zahlungsmitteln,

– Computerkriminalität,

– Korruption,

– illegaler Handel mit Waffen, Munition und Sprengstoffen,

– illegaler Handel mit bedrohten Tierarten,

– illegaler Handel mit bedrohten Pflanzenarten und -sorten,

– Umweltkriminalität, einschließlich der Meeresverschmutzung durch Schiffe,

– illegaler Handel mit Hormonen und anderen Wachstumsförderern,

– sexueller Missbrauch und sexuelle Ausbeutung, einschließlich Darstellungen von Kindesmissbrauch und Kontaktaufnahme zu Kindern für sexuelle Zwecke,

– Völkermord, Verbrechen gegen die Menschlichkeit und Kriegsverbrechen.

Die in diesem Anhang genannten Formen der Kriminalität werden von den zuständigen Behörden Neuseelands nach dem neuseeländischen Recht beurteilt.

ANHANG II – ZUSTÄNDIGE NEUSEELÄNDISCHE BEHÖRDEN UND IHRE BEFUGNISSE

Die zuständigen neuseeländischen Behörden, an die Europol Daten übermitteln kann, sind die folgenden:

Behörde
New Zealand Police (neuseeländische Polizei; als wichtigste zuständige Behörde)
New Zealand Customs Service P.O. (neuseeländische Zollbehörde)
New Zealand Immigration Service (neuseeländische Einwanderungsbehörde)

ANHANG III – LISTE DER UNIONSEINRICHTUNGEN

Einsätze/Operationen im Rahmen der Gemeinsamen Sicherheits- und Verteidigungspolitik, beschränkt auf Strafverfolgungsmaßnahmen

Europäisches Amt für Betrugsbekämpfung (OLAF)

Europäische Agentur für die operative Zusammenarbeit an den Außengrenzen (Frontex)

Europäische Zentralbank (EZB)

Europäische Staatsanwaltschaft (EUStA)

Agentur der Europäischen Union für justizielle Zusammenarbeit in Strafsachen (Eurojust)

Amt der Europäischen Union für geistiges Eigentum (EUIPO)

ANHANG IV – NATIONALE KONTAKTSTELLE

Die nationale Kontaktstelle für Neuseeland, die als zentrale Kontaktstelle zwischen Europol und den zuständigen neuseeländischen Behörden fungiert, ist die

New Zealand Police.

Neuseeland ist verpflichtet, Europol über Änderungen in Bezug auf die Kontaktstelle in Kenntnis zu setzen.