

# Liechtensteinisches Landesgesetzblatt

Jahrgang 2013

Nr. 406

ausgegeben am 17. Dezember 2013

---

## Vereinbarung zwischen dem Fürstentum Liechtenstein und dem Europäischen Polizeiamt über Geheimhaltung und Informationssicherheit

Abgeschlossen in Luxemburg am 7. Juni 2013

Zustimmung des Landtags: 3. Oktober 2013<sup>1</sup>

Inkrafttreten: 2. Dezember 2013

Das Fürstentum Liechtenstein (im Folgenden "Liechtenstein" genannt) und das Europäische Polizeiamt (im Folgenden "die Parteien" benannt), in Anbetracht dessen, dass die Parteien Kooperationsbeziehungen hergestellt haben, um die Mitgliedstaaten der Europäischen Union und Liechtenstein bei der Verhütung und Bekämpfung des organisierten Verbrechens, des Terrorismus und sonstiger Formen der internationalen Kriminalität zu unterstützen, indem sie ein Abkommen über operative Kooperation am 7. Juni 2013 (im Folgenden "Abkommen" genannt) abgeschlossen haben, im Bewusstsein der Notwendigkeit, Informationen, ob als Verschlusssache eingestuft oder nicht, die zwischen den Parteien auf der Grundlage des Abkommens ausgetauscht werden, zu schützen und zu gewährleisten, unter Berücksichtigung des Art. 19 des Abkommens, welches die Parteien verpflichtet, spezifische Standards der Geheimhaltung aufrechtzuerhalten, unter Berücksichtigung des Art. 20 des Abkommens, welches die Parteien verpflichtet, die Grundsätze nach Art. 19 des Abkommens umzusetzen, indem eine Vereinbarung abgeschlossen wird, welche insbesondere Bestimmungen über die Sicherheitsorganisation der Parteien sowie über Ausbildung, Standards zur Sicherheitsüberprüfung, die Äquivalenztabelle, die

Handhabung von Verschlusssachen und die Werte der Informationssicherheit umfasst,

in Anbetracht dessen, dass der Austausch von Informationen, die als Verschlusssache eingestuft sind, vom Inkrafttreten dieser Vereinbarung über Geheimhaltung abhängig ist,

sind wie folgt übereingekommen:

#### Art. 1

##### *Zweck*

Zweck dieses Abkommens ist die Regulierung des Schutzes von Informationen, die zwischen den Parteien ausgetauscht werden, indem die Grundsätze nach Art. 19 des Abkommens umgesetzt werden.

#### Art. 2

##### *Begriffsbestimmungen*

Im Sinne dieser Vereinbarung bezeichnet:

- a) "Informationen" in jeglicher Form kommuniziertes Wissen, das personenbezogene und/oder nicht personenbezogene Daten umfassen kann;
- b) "Verschlusssache" alle Informationen, die gegen unerlaubte Weitergabe geschützt werden müssen und entsprechend gekennzeichnet worden sind;
- c) "Geheimhaltungsgrad" die Sicherheitskennzeichnung eines Dokuments, welche die auf die Informationen anzuwendenden Sicherheitsmassnahmen bezeichnet;
- d) "Informationssystem" alle infrastrukturellen, organisatorischen, personellen und technischen Komponenten für die Erhebung, Verarbeitung, Speicherung, Übermittlung, Darstellung, Verbreitung, Zurverfügungstellung und Löschung von Informationen nach dieser Vereinbarung;
- e) "Risikobewertung" einen strukturierten Prozess für die Prüfung der informationssicherheitsrelevanten Bedrohungen, Sicherheitslücken und Auswirkungen auf das Geschäft infolge des Verlustes der Geheimhaltung, der Integrität und/oder der Verfügbarkeit von Informationen oder eines Informationssystems, um festzustellen, ob zusätzliche Sicherheitskontrollen erforderlich sind;
- f) "Akkreditierung" den Prozess, der durchgeführt wird, um zu versichern, dass alle angemessenen Sicherheitsmassnahmen umgesetzt worden sind und dass ein ausreichender Schutzgrad der Verschlusssachen und des

Informationssystems nach Massgabe dieser Vereinbarung erreicht worden ist. Der Akkreditierungsprozess bestimmt den maximalen Geheimhaltungsgrad der Informationen, die in einem Informationssystem gehandhabt werden, sowie die entsprechenden Geschäftsbedingungen;

- g) "sicherheitsrelevanter Vorfall" eine einzige oder eine Reihe von unerwünschten oder unerwarteten Informationssicherheits-Ereignissen, bei denen eine signifikante Wahrscheinlichkeit besteht, dass der Geschäftsbetrieb kompromittiert und die Informationssicherheit gefährdet wird;
- h) "Prüfung" einen strukturierten Prozess der Untersuchung, Überprüfung, Evaluierung und Berichterstattung betreffend die Verwendung der Informationen oder des Informationssystems durch eine oder mehrere sachkundige Personen, die von den zu prüfenden Situationen, Systemen, Prozessen, Funktionen usw. unabhängig sind.

## Kapitel 1 Geheimhaltung

### Art. 3

#### *Grundsätze*

Jede Partei:

1. schützt und gewährleistet Informationen nach dem Abkommen und dieser Vereinbarung, die nicht als Verschlussache eingestuft sind, mit Ausnahme der ausdrücklich als öffentlich zugänglich gekennzeichneten oder als solche eindeutig erkennbaren Informationen, durch verschiedene Massnahmen; hierzu gehören die Schweige- und Geheimhaltungspflicht, die Beschränkung des Zugangs auf das befugte Personal sowie allgemeine technische und verfahrensrechtliche Massnahmen;
2. schützt und gewährleistet Informationen nach dem Abkommen und der Vereinbarung, die als Verschlussache eingestuft sind, gemäss den folgenden Bestimmungen.

## Art. 4

*Sicherheitsorganisation*

Jede Partei stellt sicher, dass sie eine Sicherheitsorganisation, einen Sicherheitsrahmen und Sicherheitsmassnahmen zur Verfügung hat. Die Parteien stellen sicher, dass:

1. die Sicherheitsorganisation die Rollen umfasst, die mit Verantwortung für die Sicherheit auf verschiedenen Hierarchiestufen betraut werden;
2. die Inhaber der Informationen identifiziert sind;
3. eine bezeichnete Stelle verantwortlich für die Steuerung von Informationsrisiken identifiziert wird;
4. eine bezeichnete Stelle verantwortlich für die Akkreditierung von Informationssystemen, die Verschlusssachen nach dieser Vereinbarung handhaben, identifiziert wird;
5. eine bezeichnete Stelle verantwortlich für die Sicherheit elektronischer Informationen identifiziert wird;
6. eine bezeichnete Stelle verantwortlich für die Handhabung von kryptographischem Material, falls vorhanden, identifiziert wird.

## Art. 5

*Ausbildung und Sensibilisierung*

Jede Partei stellt sicher, dass alle Mitarbeiter, welche Informationen nach dieser Vereinbarung verarbeiten, mit dem Sicherheitsrahmen im Allgemeinen vertraut sind und auf die Verfahren sensibilisiert sind, um sicherheitsrelevante Probleme melden zu können. Die Parteien stellen ferner sicher, dass Mitarbeiter, welche die sichere Konfiguration von Informationssystemen verwalten und aufrechterhalten, sowie solche mit Zugang zu Informationen angemessen ausgebildet werden und auf die Verfahren zur Meldung von Vorfällen sensibilisiert sind.

## Art. 6

*Sicherheitsüberprüfungen und Ermächtigungen*

Jede Partei stellt sicher, dass:

1. alle Personen, die in Ausübung ihrer amtlichen Tätigkeit Zugang zu Verschlusssachen haben müssen, die im Rahmen dieses Abkommens bereitgestellt oder ausgetauscht werden, oder deren Tätigkeit oder Aufgaben Zugang zu solchen Verschlusssachen bieten kann, in angemessener Weise

- sener Weise einer Sicherheitsüberprüfung unterzogen werden, bevor ihnen Zugang zu solchen Informationen gewährt wird.
2. die Verfahren der Sicherheitsüberprüfung der Feststellung dienen, ob einer Person in Anbetracht ihrer Loyalität, Vertrauenswürdigkeit und Verlässlichkeit Zugang zu Verschlussachen gewährt werden kann.
  3. die weitere Berechtigung einer Person für den Zugang zu Verschlussachen regelmässig geprüft wird.

#### Art. 7

##### *Wahl des Geheimhaltungsgrads*

1) Jede Partei ist verantwortlich für die Wahl des geeigneten Geheimhaltungsgrads für Informationen, die der anderen Partei geliefert werden.

2) Gelangt eine Partei anhand der ihr bereits vorliegenden Informationen zu dem Schluss, dass ein gewählter Geheimhaltungsgrad zu ändern ist, unterrichtet sie die andere Partei und bemüht sich, Einvernehmen über einen geeigneten Geheimhaltungsgrad zu erzielen. Ohne die schriftliche Einwilligung der anderen Partei darf keine Partei Geheimhaltungsgrade festlegen oder ändern, die sich auf von der anderen Partei gelieferte Informationen beziehen.

3) Jede Partei kann jederzeit eine Änderung des Geheimhaltungsgrads, der sich auf von ihr gelieferte Informationen bezieht, beantragen, einschliesslich einer allfälligen Aufhebung des Grads. Die andere Partei ändert den Geheimhaltungsgrad gemäss dem Antrag. Jede Partei beantragt die Einstufung in einen niedrigeren Geheimhaltungsgrad oder die Aufhebung der Geheimhaltung, sobald es die Umstände gestatten.

4) Jede Partei kann den Zeitraum, für den ein gewählter Geheimhaltungsgrad, der sich auf die von ihr gelieferten Informationen bezieht, gelten soll angeben, sowie etwaige Änderungen des Geheimhaltungsgrads für den nachfolgenden Zeitraum.

5) Sind Informationen, bei denen der Geheimhaltungsgrad geändert wird, nach Massgabe dieses Artikels an Drittparteien geliefert worden, werden alle Empfänger über die Änderung des Geheimhaltungsgrads informiert.

## Art. 8

*Äquivalenztabelle*

Die Parteien legen fest, dass die folgenden Geheimhaltungsgrade unter den nationalen Gesetzesbestimmungen Liechtensteins und die innerhalb von Europol verwendeten Geheimhaltungsgrade äquivalent sind, und sie gewähren äquivalenten Schutz für die mit diesen Geheimhaltungsgraden gekennzeichneten Informationen:

Für Liechtenstein	Für Europol
EINGESCHRÄNKT	RESTREINT UE / EU RESTRICTED
VERTRAULICH	CONFIDENTIEL UE / EU CONFIDENTIAL
GEHEIM	SECRET UE / EU SECRET

## Art. 9

*Registrierung*

Jede Partei trägt alle Informationen, die als CONFIDENTIEL UE / EU CONFIDENTIAL oder höher eingestuft werden oder die in Liechtenstein diesem Geheimhaltungsgrad entsprechen, in ihr Register ein. Die registrierten Informationen beinhalten zumindest das Minimum, welches für die eindeutige Identifizierung der entsprechenden Informationen erforderlich ist, so zum Beispiel deren Referenznummer, Gegenstand, Datum und Geheimhaltungsgrad.

## Art. 10

*Kennzeichnung*

Jede Partei stellt sicher, dass die Verschlusssachen nach dieser Vereinbarung immer eindeutig mit den in Art. 8 festgelegten Bezeichnungen gekennzeichnet werden, um eine Erkennung des Geheimhaltungsgrads zu ermöglichen.

## Art. 11

*Speicherung*

Alle Verschlusssachen nach dieser Vereinbarung werden auf eine sichere Weise gespeichert, die dem jeweiligen Rechtsrahmen der Partei entspricht.

## Art. 12

*Vervielfältigung und Übersetzung*

1) Jede Partei stellt sicher, dass Vervielfältigungen von Verschlusssachen auf eine Zahl beschränkt werden, die zur Erfüllung der wesentlichen Anforderungen unbedingt notwendig ist. Die auf die Originalinformationen anwendbaren Sicherheitsmassnahmen sind auch auf die Vervielfältigungen anwendbar.

2) Jede Partei stellt sicher, dass alle einzelnen Vervielfältigungen von Informationen, die als CONFIDENTIEL UE / EU CONFIDENTIAL oder höher eingestuft werden oder die in Liechtenstein diesem Geheimhaltungsgrad entsprechen, mit einer eindeutigen Nummer gekennzeichnet werden, welche die Identifizierung jeder einzelnen Vervielfältigung der Informationen ermöglicht.

3) Für die Zwecke dieser Vereinbarung gelten alle Übersetzungen von Verschlusssachen als Vervielfältigungen der Originalinformationen.

## Art. 13

*Versendung*

1) Verschlusssachen werden auf eine sichere Weise versandt, die dem jeweiligen Rechtsrahmen der übermittelnden Partei entspricht.

2) Informationen, die als CONFIDENTIEL UE / EU CONFIDENTIAL oder höher eingestuft werden oder die in Liechtenstein diesem Geheimhaltungsgrad entsprechen, werden zwischen den verantwortlichen Registern der Parteien ausgetauscht.

3) Die Versendung von Informationen, die als CONFIDENTIEL UE / EU CONFIDENTIAL eingestuft werden, wird von den verantwortlichen Registern dokumentiert.

4) Der Empfang von Verschlusssachen wird bestätigt.

## Art. 14

*Vernichtung*

1) Jede Partei stellt sicher, dass nicht mehr benötigte Verschlusssachen auf eine Weise vernichtet werden, die den anwendbaren Standards entspricht, so dass eine Wiederherstellung, ganz oder teilweise, verunmöglicht wird.

2) Abfallprodukte, die aus der Erstellung von Verschlussachen hervorgehen und selbst als Verschlussachen einzustufen sind, müssen mit der gleichen Sorgfalt und auf die gleiche Weise vernichtet werden wie die Verschlussachen selbst.

3) Im Falle von Informationen, die als CONFIDENTIEL UE / EU CONFIDENTIAL oder höher eingestuft werden oder die in Liechtenstein diesem Geheimhaltungsgrad entsprechen, wird die Vernichtung durch das Register nach Massgabe des jeweiligen Rechtsrahmens der Partei registriert.

#### Art. 15

##### *Evaluationen*

Jede Partei erlaubt der anderen Partei, nach Erhalt einer schriftlichen Erlaubnis ihr Hoheitsgebiet oder ihre Räumlichkeiten zu besuchen, um ihre Verfahren und Anlagen für den Schutz von Verschlussachen, die von der anderen Partei übermittelt werden, zu evaluieren. Die Vorkehrungen für den Besuch werden bilateral vereinbart. Jede Partei unterstützt die andere Partei bei der Beurteilung, ob die von der anderen Partei zur Verfügung gestellten Verschlussachen ausreichend geschützt sind.

#### Art. 16

##### *Kompromittierung von Verschlussachen*

1) Die Sicherheitsbehörde jeder Partei meldet der Sicherheitsbehörde der anderen Partei sofort jede mögliche Kompromittierung von Verschlussachen.

2) Im Falle einer unberechtigten Offenlegung arbeiten beide Parteien in angemessener Weise bei der Ermittlung zusammen und informieren einander über die Resultate.

### Kapitel 2

## Informationssicherheit

#### Art. 17

##### *Informationssicherheitspolitik*

Als Teil ihrer übergreifenden Sicherheitspolitik hat jede Partei eine Informationssicherheitspolitik zur Verfügung, die festlegt, wie sie und ihre

Lieferungspartner die Mindestanforderungen gemäss dieser Vereinbarung erfüllen.

#### Art. 18

##### *Steuerung von Informationsrisiken*

Jede Partei führt regelmässig Informationsrisikobeurteilungen durch sowie - wenn sich eine Risikokomponente (Bedrohung, Sicherheitslücke, Auswirkungen usw.) wesentlich verändert - Beurteilungen der betriebenen Informationssysteme. Die Entscheide, die im Rahmen der Evaluierung und der Risikosteuerung gefällt werden, werden in der relevanten Risikosteuerungs-Dokumentation registriert.

#### Art. 19

##### *Akkreditierung*

Jede Partei stellt sicher, dass Informationssysteme, die Verschlussachen nach dieser Vereinbarung verarbeiten, akkreditiert werden. Der Akkreditierungsstatus wird regelmässig geprüft, um zu beurteilen, ob es wesentliche Änderungen gegeben hat, die den ursprünglichen Akkreditierungsentscheid ändern könnten.

#### Art. 20

##### *Prüfung*

Jede Partei führt Sicherheitsprüfungen von Informationssystemen durch, die Verschlussachen nach dieser Vereinbarung verarbeiten.

#### Art. 21

##### *Identity and Access Management*

Jede Partei hat geeignete Identifizierungs- und Authentifizierungskontrollen für Informationssysteme zur Verfügung, die Verschlussachen nach dieser Vereinbarung verarbeiten.

#### Art. 22

##### *Kryptographie*

Jede Partei verwendet kryptographische Kontrollen für den sicheren Austausch von Verschlussachen nach dieser Vereinbarung. Kryptographi-

sche Geräte werden nach Massgabe des Rechtsrahmens der übermittelnden Partei bewilligt.

#### Art. 23

##### *Abhören und elektromagnetische Gegenmassnahmen*

Informationssysteme, welche Informationen handhaben, die als CONFIDENTIEL UE / EU CONFIDENTIAL oder höher eingestuft werden oder die in Liechtenstein diesem Geheimhaltungsgrad entsprechen, werden auf der Grundlage einer Risikobeurteilung so geschützt, dass die Informationen nicht durch Abhören und/oder durch elektromagnetische Ausstrahlungen kompromittiert werden können.

#### Art. 24

##### *Meldung von Vorfällen*

Jede Partei hat klare Regeln und Verfahren zur Verfügung, um sicherheitsrelevante Vorfälle und Sicherheitsverletzungen zu melden, bewältigen und beheben.

#### Art. 25

##### *Wechseldatenträger*

Jede Partei hat Regeln und Verfahren zur Verfügung betreffend die angemessene Verwendung und den angemessenen Schutz von Wechseldatenträgern, welche zur Speicherung von Verschlusssachen nach dieser Vereinbarung verwendet werden.

#### Art. 26

##### *Sichere Entsorgung*

Jede Partei stellt sicher, dass alle Medien und Datenträger, welche für die Speicherung oder die Verarbeitung von Verschlusssachen verwendet werden, nach Massgabe des jeweiligen Rechtsrahmens der Partei sicher entsorgt oder gelöscht werden.

## Kapitel 3

# Schlussbestimmungen

### Art. 27

#### *Inkrafttreten*

Diese Vereinbarung tritt am ersten Tag des Monats nach erfolgter Unterzeichnung durch die letzte Partei in Kraft, auf jeden Fall aber nicht bevor das Abkommen in Kraft getreten ist.

Der Austausch von Informationen, die als Verschlussache eingestuft sind, erfolgt erst nach dem Inkrafttreten dieser Vereinbarung.

### Art. 28

#### *Änderungen und Beendigung*

1) Diese Vereinbarung kann jederzeit im gegenseitigen Einvernehmen der Parteien schriftlich geändert werden.

2) Diese Vereinbarung kann von jeder Partei mit einer Kündigungsfrist von drei Monaten beendet werden. In diesem Falle bleiben die Rechtswirkungen dieser Vereinbarung in Kraft.

3) Diese Vereinbarung tritt automatisch an dem Tag ausser Kraft, an dem das Abkommen beendet wird.

Geschehen zu Luxemburg am 7. Juni 2013 in doppelter Ausfertigung in deutscher und englischer Sprache, wobei jeder Wortlaut gleichermaßen verbindlich ist.

Für das  
Fürstentum Liechtenstein:

Für Europa:

gez. Dr. Thomas Zwiefelhofer

gez. Rob Wainwright

1 *Bericht und Antrag der Regierung Nr. [65/2013](#)*