

Liechtensteinisches Landesgesetzblatt

Jahrgang 2018

Nr. 4

ausgegeben am 25. Januar 2018

Verordnung

vom 23. Januar 2018

betreffend die Abänderung der Verordnung über elektronische Kommunikationsnetze und -dienste

Aufgrund von Art. 52a Abs. 4, Art. 52b Abs. 6 und Art. 76 des Gesetzes vom 17. März 2006 über die elektronische Kommunikation (Kommunikationsgesetz; KomG), LGBI. 2006 Nr. 91, in der geltenden Fassung, verordnet die Regierung:

I.

Abänderung bisherigen Rechts

Die Verordnung vom 3. April 2007 über elektronische Kommunikationsnetze und -dienste (VKND), LGBI. 2007 Nr. 67, in der geltenden Fassung, wird wie folgt abgeändert:

Art. 1 Abs. 2 Bst. h

Aufgehoben

Art. 2 Abs. 1 Bst. x und y

- 1) Im Sinne dieser Verordnung bedeutet:
- x) "Betriebsdaten": Teilnehmer-, Verkehrs- und Standortdaten, soweit diese für den Anbieter für die in Art. 51, 52 und 54 erfassten Zwecke notwendig sind;

- y) "Vorratsdatenbank": eine Datenbank zur Speicherung von Vorratsdaten.

Art. 8 Abs. 2 Bst. a

Aufgehoben

Art. 19 Bst. f

Aufgehoben

Art. 54a Abs. 1 Einleitungssatz und Bst. d Ziff. 1, Abs. 2 und 3

1) Folgende Datenkategorien müssen von Anbietern nach Art. 52a des Gesetzes auf Vorrat gespeichert werden:

d) zur Bestimmung der Art einer Nachrichtenübermittlung benötigte Daten:

1. betreffend Telefonfestnetz und Mobilfunk: der in Anspruch genommene Telefondienst;

2) Anbieter dürfen keinerlei Daten, die Aufschluss über den Inhalt einer Kommunikation geben, auf Vorrat speichern.

3) Alle auf Vorrat gespeicherten Daten müssen unbeschadet des Art. 49 Abs. 2 des Gesetzes sechs Monate ab dem Zeitpunkt der Beendigung des Kommunikationsvorganges binnen sieben Tagen und unwiderruflich gelöscht werden.

Art. 54b Abs. 1 und 2 Einleitungssatz und Bst. a

1) Die Datenschutzstelle ist zuständig für die Überwachung der Einhaltung der Grundsätze der Datensicherheit, die Erstellung einer Statistik über die Speicherung von Vorratsdaten sowie die jährliche Berichterstattung an den Landtag.

2) Anbieter nach Art. 52a des Gesetzes sind verpflichtet, der Datenschutzstelle die Auskünfte zu erteilen, die für die Erfüllung ihrer Aufgaben, insbesondere der jährlichen Berichterstattung, notwendig sind. Dies sind insbesondere Auskünfte darüber:

- a) in welchen Fällen im Einklang mit den Bestimmungen der Strafprozessordnung Daten an die zuständigen Behörden weitergegeben worden sind;

Überschriften vor Art. 60

VIII. Mitwirkung und Datenbekanntgabe

A. Allgemeine Bestimmungen

Art. 60 Abs. 1, 3 und 4

1) Anbieter sind verpflichtet, täglich während 24 Stunden zur Mitwirkung und Auskunftserteilung nach Art. 51 bis 53 des Gesetzes zur Verfügung zu stehen.

3) Aufgehoben

4) Auf die Entschädigung für die Mitwirkung bei einer Standortfeststellung nach Art. 51 des Gesetzes oder einer Auskunftserteilung nach Art. 52a des Gesetzes finden die Art. 65 bis 68 sinngemäss Anwendung; die Entschädigung ist bei der ersuchenden Behörde geltend zu machen.

Art. 61 Abs. 1 Bst. d

- 1) Die Reaktionszeit für die Bereitstellung der entsprechenden Daten im Rahmen der Mitwirkung und Auskunftserteilung beträgt höchstens:
d) 24 Stunden bei Vorratsdaten nach Art. 52a des Gesetzes.

Überschrift vor Art. 68a

C. Datensicherheit bei der Vorratsdatenspeicherung

Art. 68a

Datensicherheit beim Anbieter innerhalb des Betriebes

1) Vorratsdaten müssen vom Anbieter auf eine Weise gespeichert werden, dass deren logische Unterscheidung von Betriebsdaten bei jedem Zugriff und jeder Verwendung eindeutig ist.

2) Eine physikalisch getrennte Datenspeicherung von Betriebsdaten und Vorratsdaten ist nicht notwendig. Der Anbieter hat durch geeignete technische und organisatorische Massnahmen sicherzustellen, dass die Vorratsdatenbank auf eine Weise ausgestaltet ist, dass Zugriffe auf Vorratsdaten nur unter Einhaltung der besonderen Sicherheitsvorschriften nach Art. 68b und 68c möglich sind.

3) Wenn keine betriebliche Rechtfertigung zur Speicherung als Betriebsdaten mehr vorliegt, sind diese Daten umgehend aus den betrieblichen Datenbanken zu löschen und in die Vorratsdatenbank zu überführen. Sollte die Speicherung in der Vorratsdatenbank bereits zuvor erfolgt sein, so ist die Kennzeichnung der gleichzeitigen betrieblichen Speicherung zeitgleich oder unmittelbar nach der Löschung aus den betrieblichen Datenbanken zu entfernen.

4) Der Anbieter hat die Methode zur technischen und organisatorischen Trennung nachvollziehbar zu dokumentieren und diese Dokumentation für den Fall einer Prüfung durch die Datenschutzstelle nach Art. 52b des Gesetzes zugänglich zu machen.

5) Der Anbieter hat die tatsächliche Speicherdauer von Betriebsdaten sowie allfällige diesbezügliche interne Richtlinien für den Fall einer Prüfung durch die Datenschutzstelle bekanntzugeben.

Art. 68b

Revisionssichere Protokollierung und Vier-Augen-Prinzip bei der Bearbeitung von Vorratsdaten

1) Der Anbieter hat seine Systeme auf technischer und organisatorischer Ebene so auszugestalten, dass die Bearbeitung von Vorratsdaten nur durch besonders ermächtigte Mitarbeiter unter Einhaltung des Vier-Augen-Prinzips möglich ist. Jede Bearbeitung von Vorratsdaten muss durch zwei Personen mit einer besonderen Ermächtigung hierfür autorisiert sein. Die Autorisierung durch die zweite Person kann auch zeitnah zur Bearbeitung durch die erste Person nachträglich erfolgen, wenn dabei die effektive Wahrung des Vier-Augen-Prinzips sichergestellt ist.

2) Die Bearbeitung von Vorratsdaten im Fall einer gerichtlichen Anordnung nach § 102a StPO muss beim Anbieter so protokolliert werden, dass die Protokolldaten vor Veränderung und Verfälschung geschützt sind und die Vollständigkeit, die Ordnungsmässigkeit, die Sicherung vor Verlust, die Einhaltung der Aufbewahrungsfristen sowie die Dokumentation, Nachvollziehbarkeit und Prüfbarkeit des Verfahrens gewahrt sind.

3) Die Protokollierung ist auf einem von der Datenschutzstelle herauszugebenden Formular vorzunehmen.

Art. 68c

Transport- und Inhaltsverschlüsselung

1) Für die Übermittlung von Vorratsdaten an Strafverfolgungsbehörden ist eine Verschlüsselung (Transportverschlüsselung) vorzusehen.

2) Zusätzlich ist eine Verschlüsselung der Inhalte sowohl der Anfrage als auch der Beantwortung von Absender zu Empfänger durch asymmetrische Verschlüsselungsverfahren vorzusehen (Inhaltsverschlüsselung). Asymmetrische Verschlüsselungsverfahren können als hybride Verfahren implementiert werden.

Anhang 1 Ziff. XVI, XVII und XVIII

Aufgehoben

Anhang 2 Ziff. III

Aufgehoben

II.

Inkrafttreten

Diese Verordnung tritt am 1. Februar 2018 in Kraft.

Fürstliche Regierung:
gez. *Dr. Daniel Risch*
Regierungschef-Stellvertreter