1. Grundzüge des Entwurfs

Grundsätzlich verfolgt der Entwurf das Ziel, die Richtlinie so umzusetzen, dass zwar ihr Zweck – die Ermittlung, Feststellung und Verfolgung von schweren Straftaten mittels auf Vorrat gespeicherter personenbezogener Daten – innerstaatlich erreicht wird, um den Strafverfolgungsbehörden die Verwendung zeitgemäßer technischer Mittel zu ermöglichen, zugleich aber durch gesetzliche Vorkehrungen sichergestellt ist, dass

- die mit der Vorratsdatenspeicherung verbundenen Grundrechtseingriffe so gering wie möglich – und damit verhältnismäßig zum verfolgten Zweck – ausfallen,
- die Sicherheit der Daten sowohl bei den Telekommunikationsbetreibern als auch bei den zur Datenanwendung berechtigten Behörden bestmöglich gewährleistet ist,
- den datenschutzrechtlich erforderlichen Informationspflichten nachgekommen wird,
- alle notwendigen Rechtsmittel zur Verfolgung der datenschutzrechtlichen und grundrechtlichen Interessen Betroffener zur Verfügung stehen,
- darüber hinausgehende unabhängige datenschutzrechtliche Kontrollen vorgesehen werden, und
- die wirtschaftlichen Auswirkungen der Vorratsdatenspeicherung auf die zur Speicherung und Auskunft verpflichteten Telekommunikationsbetreiber grundrechtskonform zu gestalten.

Der Entwurf sieht vor, dass über die schon bisher für Telekommunikationsbetreiber bestehende Berechtigung zur Speicherung und Verarbeitung von Daten für betriebsnotwendige, insbesondere für Verrechnungszwecke (in der Regel für einen Zeitraum von drei Monaten) hinaus in Umsetzung der Vorgaben der Richtlinie bestimmte, näher umschriebene Daten (insbesondere IP-Adressen und Standortdaten) ab dem Zeitpunkt der Erzeugung oder Verarbeitung bis sechs Monate nach Beendigung der Kommunikation zu speichern sind (vorgeschlagener § 102a TKG). Der Begriff „Vorratsdaten“ stellt keine neue Kategorie im Sinne von Verkehrsdaten, Standortdaten, Inhaltsdaten oder Stammdaten dar, sondern stellt vielmehr auf den Zweck ab, für den die Daten von den Telekommunikationsanbietern gesammelt werden müssen.

Nach dem Entwurf dürfen Verkehrsdaten außer in den im TKG geregelten Fällen weder gespeichert noch verwendet werden und sind vom Betreiber nach Beendigung der Verbindung unverzüglich zu löschen oder zu anonymisieren (vorgeschlagener § 99 TKG). Mit dieser nun auch vom Wortlaut ausdrücklich abschließenden Regelung soll insoweit Rechtssicherheit geschaffen werden, als damit aus anderen gesetzlichen Bestimmungen weder eine Berechtigung noch gar eine Verpflichtung zur Speicherung von Verkehrsdaten abgeleitet werden kann.

Von der Speicherpflicht nicht erfasst sind Unternehmen, die mittels Bescheid als kleines Unternehmen gemäß der Empfehlung der EU Kommission 2003/361/EG eingestuft werden (vorgeschlagener § 102a Abs. 6 TKG). Diejenigen Telekommunikationsanbieter, die zur Speicherung verpflichtet sind, gelten zur rechtlichen Klarstellung in Bezug auf Vorratsdaten als Auftraggeber des öffentlichen Bereits (vorgeschlagener § 102a Abs. 9 TKG). Die den

Anbietern aus der Umsetzung der Vorratsdatenspeicherung entstehenden Kosten werden entsprechend vergütet (vorgeschlagener § 94 TKG).

Die auf Vorrat gespeicherten Daten dürfen ausschließlich aufgrund einer gerichtlichen Bewilligung und nur nach Maßgabe ausdrücklicher Gesetzesbestimmungen, die auf § 102a Bezug nehmen, zum Zweck der Ermittlung, Feststellung und Verfolgung von schweren Straftaten an die nach der StPO zuständigen Behörden übermittelt werden (vorgeschlagener § 102b TKG).

So wie bisher haben die zuständigen Behörden nach der StPO zur Verfolgung „niederschwelliger“ Straftaten (also solcher, die keine „schweren Straftaten“ sind) das Recht auf Beauskunftung der bei den Telekommunikationsbetreibern für betriebsnotwendige Zwecke gespeicherten Verkehrsdaten, wenn eine gerichtliche Bewilligung vorliegt (vorgeschlagener § 99 Abs. 5 Z. 1 TKG).

Ebenso wie bisher sind die nach dem SPG zuständigen Sicherheitsbehörden für die Erfüllung ihrer im SPG geregelten präventiven Aufgaben berechtigt, Auskünfte über die bei den Telekommunikationsbetreibern für betriebsnotwendige Zwecke gespeicherten Daten einzuholen. Darüber hinaus sieht eine Verfassungsbestimmung vor, dass Sicherheitsbehörden für die Abwehr einer konkreten Gefahr für das Leben oder die Gesundheit eines Menschen unter bestimmten engen Voraussetzungen Auskünfte über Stammdaten und Standortdaten auch dann erhalten können, wenn dafür die Verwendung von Verkehrsdaten notwendig ist und deshalb in das unter Richtervorbehalt stehende Fernmeldegeheimnis eingegriffen wird (vorgeschlagener § 99 Abs. 5 Z. 2 TKG).

Neben der positivrechtlichen Definition von einigen neuen, insbesondere technischen Begriffen beinhaltet der Entwurf die Definition, wie die IP-Adresse rechtlich einzuordnen ist. Entsprechend den jüngsten Entscheidungen des OGH wie auch des VwGH wird die IP-Adresse als Zugangsdatum und damit als Verkehrsdatum qualifiziert, wodurch sie in den Schutzbereich des Fernmelde- wie auch des Kommunikationsgeheimnisses fällt (vorgeschlagener § 92 Abs. 3 Z 16 TKG).

Der Entwurf sieht eine Trennung zwischen für betriebsnotwendige Zwecke und auf Vorrat gespeicherte Daten vor, für deren Speicherung besondere Sicherungsmaßnahmen vorgesehen sind. Die Kontrolle wird der Datenschutzkommission übertragen (vorgeschlagener § 102c Abs. 1 TKG). Jeder Zugriff auf Vorratsdaten ist zudem zu protokollieren (vorgeschlagener § 102c Abs. 2 und 3 TKG). Die Beauskunftung von Daten einer Nachrichtenübermittlung nach den Bestimmungen der StPO wie auch die Beauskunftung solcher Daten an die Sicherheitsbehörden hat verschlüsselt zu erfolgen (vorgeschlagener § 94 Abs. 4 TKG).

Schließlich sieht der Entwurf entsprechende neue Verwaltungsstraftatbestände vor (vorgeschlagener § 109 TKG).