

## Ludwig Boltzmann Institut für Menschenrechte (BIM)



A - 10 10 Wien  
Freyung 6, 1. Hof, Stiege II  
Tel. +43 (1) 4277 / 27420  
Web: <http://bim.lbg.ac.at>  
Email: [bim.staatsrecht@univie.ac.at](mailto:bim.staatsrecht@univie.ac.at)



Ein Institut der  
Ludwig Boltzmann Gesellschaft

# Vorratsdatenspeicherung Die Umsetzung in Österreich im Finale

ISPA ACADEMY

14.12.2011

Ing. Mag. Christof Tschohl  
Wissenschaftlicher Mitarbeiter des BIM



Ludwig Boltzmann Institut für Menschenrechte (BIM)

## Hintergrund I Die Beauftragung des BIM

- **Anfrage des BMVIT im Februar 2009**
  - Vertragsverletzungsverfahren eingeleitet (Zeitdruck)
  - BIM hat Erfahrung und Überblick durch die Studie zur VDS 2008
  - Kombination Technik und Recht
  - neutrale Institution, die alle betroffenen Kreise einbinden soll
  
- **Kritik an der Beauftragung des BIM**
  - seitens BM.I und BMJ: Bekannte Kritiker der RL („Bock zum Gärtner“)
  - seitens Zivilgesellschaft (NGO's): Menschenrechts-Institut als „Feigenblatt“



Ludwig Boltzmann Institut für Menschenrechte (BIM)

## Hintergrund II Der Zugang des BIM

### VDS ist an sich nicht vereinbar mit Grundrechten !!

- Anfechtung nach der Umsetzung gegenüber BMVIT vorbehalten – auch gegen Normen gemäß BIM-Vorschlag
- „Schadensbegrenzung“: Art der Umsetzung entscheidet Schwere des Eingriffs
- Einbindung ALLER Beteiligten (auch Zivilgesellschaft)
- Umsetzung muss „Gesamtpaket“ im Auge haben - nicht nur TKG, auch StPO und SPG
- BIM liefert Entwurf für TKG-Novelle – öffentliche Kritik am Ergebnis der politischen Umsetzung bleibt vorbehalten



Ludwig Boltzmann Institut für Menschenrechte (BIM)

## Hintergrund III

### Chancen zur „Schadensbegrenzung“

#### Oder: Warum hat das BIM den Auftrag angenommen?

- Die VDS-Umsetzung legt Probleme offen, die schon lange ungelöst sind (zB IP-Adressen)
- Die wesentlichsten Datenschutzprobleme sind nicht neu
- Datenschutzteil des TKG war schon ohne VDS reparaturbedürftig
- Die mangelhafte Determinierung der RL 2006/24/EG ist bei der Umsetzung grundrechtsfreundlich zu beheben
- Grundrechtsschutz durch technisch enge Determinierung schon im Gesetz
- Grundrechtsschutz durch technische Umsetzung („Privacy by Design“)



Ludwig Boltzmann Institut für Menschenrechte (BIM)

## I. Grundzüge BIM-Entwurf

- „Vorratsdaten“ keine neue Kategorie (iSv Verkehrsdaten, Inhaltsdaten, Stammdaten)  
→ Unterscheidung bezogen auf den Zweck (§ 92 Abs 3 Z 6b; § 102a)
- Verwendungszwecke der Daten im TKG abschließend geregelt (Rechtssicherheit)  
→ keine Berechtigung /Verpflichtung zur Speicherung aus anderen Normen (§ 99 Abs 1)
- kleine Unternehmen nicht speicherpflichtig  
→ ZB Internet Cafe, WLAN für Kunden (administrativ/wirtschaftlich unverhältnismäßig)
- Kosten der technischen Umsetzung zu einem angemessenen Teil vom Bund zu tragen  
→ VfGH Judikatur zum Investitionskostenersatz für „legal interception“, § 94)
- Einschränkung der Speicherpflicht auf Ebene der technischen Definitionen:  
→ Öffentliche IP-Adresse, keine NAT/PAT Events, keine Portspeicherung, E-Mail nur auf SMTP Basis, keine historischen E-Mail Aliases, etc.
- Eigene Bestimmung zu Datensicherheit und Protokollierung (§ 102c TKG)
- Definition der Schnittstelle („Technische Richtlinie“) per Verordnung  
→ aber durch § 94 Abs. 4 TKG eng determiniert



Ludwig Boltzmann Institut für Menschenrechte (BIM)

## II. Grundzüge BIM-Entwurf – Verwendungszwecke

- **Übermittlung von Vorratsdaten:**
  - gerichtliche Bewilligung
  - nur für Ermittlung, Feststellung und Verfolgung schwerer Straftaten nach der StPO
  - „Betriebsdaten“ nach wie vor verfügbar (§ 99 Abs 5 Z1)
- **Sonderproblem IP-Adressen: Verkehrs- oder Stammdaten?**

OGH 14.7.2009 (LSG gg Tele2, 4Ob41/09x), **Rechtssatz:** „Dynamische, dh nur für eine bestimmte Zeit zugewiesene IP-Adressen sind in die Kategorie der Zugangs- und damit der Verkehrsdaten einzuordnen.“

**Obiter Dictum:** IP-Logs dürften gar nicht so lange gespeichert werden;  
**VwGH 27.05.2009 zu GZ 2007/05/0280 :** Fernmeldegeheimnis des Art 10a StGG für IP-Adressen anwendbar → Richtervorbehalt!

  - Definition nach TKG-Entwurf: IP-Adressen = Zugangsdaten
  - (statische IP-Adressen sind zugleich Stammdaten und Zugangsdaten - Doppelnatur)
  - bereinigt Judikaturdivergenz zwischen Zivil- (4Ob41/09x) und Strafsenat (11 Os 57/05)
  - Konsequenz: IP-Logs sind nur wenige Tage/Wochen im Live-System beim Provider notwendig/vorhanden, danach Vorratsdaten mit allen Einschränkungen (schwere Straftat, Protokollierung, Zugriffsbeschränkung für den Anbieter selbst)



Ludwig Boltzmann Institut für Menschenrechte (BIM)

## Kritik an der TKG-Novelle

- Richtervorbehalt wurde „durchlöchert“ (Ausnahmen in § 99 Abs. 5 TKG)
- Anbieter sind nicht wie im BIM-Entwurf datenschutzrechtliche Auftraggeber des öffentlichen Bereichs bzgl. Vorratsdaten
- Begriff „schwere Straftaten“ kommt nirgends mehr vor – Etikettenschwindel: „Straftat, deren Schwere eine Anordnung nach § 135 Abs. 2a StPO rechtfertigt“ – im Endeffekt die gleich Voraussetzungen wie bisher (Strafdrohung 1 Jahr+)
- Keine automatische Verständigung durch den Anbieter bei Standortdaten-Auskünften für Zwecke der ersten allgemeinen Hilfeleistung (§ 53 Abs. 3b SPG)
- Für IP-Adressen Auskünfte gibt es gar keine Strafdrohungsgrenzen (§ 76a StPO)
- Ausnahmen vom Richtervorbehalt in § 99 Abs. 5 Z 2 TKG sind viel zu weit (auch passiver E-Mail Verkehr, IMSI, IMEI) → allerdings wieder eingeschränkt durch § 76a Abs. 2 StPO (Grund: Änderungen erst in zweiter Lesung im Nationalrat beschlossen, auch NAT/PAT)
- Informationspflicht gegenüber Betroffenen nach SPG nur dann, wenn Vorratsdaten betroffen sind (sachlich nicht begründbar) – nach wie vor kein 4 Augen Prinzip im SPG



Ludwig Boltzmann Institut für Menschenrechte (BIM)

## Kriterien zur Beurteilung der Speicherpflicht

- **Eigenschaft des Anbieters**
  - Gewerblicher Dienstanbieter im Sinne des TKG?
    - wenn der Dienst nur unselbständiger Bestandteil eines sonstigen Gewerbes ist besteht keine Speicherpflicht (zB Hotel mit W-LAN Hotspot)
  - Beitragspflicht nach § 34 KommAustriaG? → Ausnahme kleiner Anbieter
  - Netzbetreiber oder Dienstanbieter (Wholesale)?
    - Speicherpflicht trifft nur Dienstanbieter – jeder muss nur Speichern, was er selber an Daten erzeugt oder verarbeitet (§ 102a Abs. 5 TKG)
- **Art des Kommunikationsdienstes**
  - Öffentlicher Dienst? → keine unternehmens- oder konzerninternen Systeme – Abgrenzung funktionell: Wenn zB ein E-Mail den internen Bereich verlässt und über den öffentlichen Mailserver nach außen geht, besteht die Speicherpflicht nur bzgl. des öffentlichen Knotens
  - Abgrenzung „intern/extern“: funktionell, organisatorisch, technisch (zB private IP)
  - Kein bloßer Dienst der Informationsgesellschaft (vgl. § 3 TKG) – zT Überschneidungen
- **Technisch**
  - Bei E-Mail nur SMTP basiert; bei Internet Zugang nur öffentliche IP-Adressen



Ludwig Boltzmann Institut für Menschenrechte (BIM)

## „Ideengeschichte“ der Schnittstelle

### Ausgangsüberlegung zur Grundrechtsbedrohung:

- Eine komplexe Schnittstelle zwischen Sicherheitsbehörden und Anbieter ermöglicht uU mehr als die RL erlaubt
- 2009 existierte bereits die Spezifikation einer ETSI-Schnittstelle zur Vorratsdatenspeicherung (umgesetzt zB in Deutschland, GB, uvm)
- ETSI-Schnittstelle lässt Datamining zu → eigentlich eine integrierte „IKT-Rasterfahndung“
- ETSI-Schnittstelle harmonisiert die Datenbestände aller Anbieter so weit, dass logisch eine zentrale staatliche Datenspeicherung vorliegt
- Auskünfte laufen automatisiert (zB GB) – keine echte Kontrolle durch den Anbieter mehr
- BMI und BMJ hatten bereits die ETSI-Schnittstelle gefordert – trotz immenser Kosten auch auf staatlicher Seite



Ludwig Boltzmann Institut für Menschenrechte (BIM)

## Strategie zur „ETSI-Prävention“

### Von Beginn an Ausgangsbasis im Konzept des BIM:

- Die politische Forderung soll mit konstruktiven konkreten Vorschlägen gebändigt werden → erfordert Nachweis der Machbarkeit, soll Kostengünstiger und trotzdem fortschrittlich sein
- Im BIM Konzept am Anfang (Frühsommer 2009) daher die Idee: Festlegung im TKG auf CSV-File

### Vorteile des CSV-Konzepts:

- Automatisierung der Abfrage beim Anbieter nicht zwingend – aber für den Anbieter nach eigener Gestaltung möglich (keine Harmonisierung)
- „Use-Cases“ werden statisch auf die gesetzlich zulässigen Fälle festgelegt (kein Dataming)
- Technikneutral, Kostengünstig, interoperabel



Ludwig Boltzmann Institut für Menschenrechte (BIM)

## Erstes Konzept zur Schnittstelle

### Arbeitsgruppen BIM + Anbieter im Sommer 2009:

- Parallel zur Definition der betroffenen Daten beginnen die Überlegungen zur Schnittstelle – Einigkeit gegen ETSI-Standard
- Anregung des BIM: Die Telekom-Branche soll so schnell wie möglich von sich aus einen Vorschlag für eine „Technische Richtlinie“ erarbeiten und Vorlegen → Einigkeit, Machbarkeit und rasche Umsetzbarkeit als Argument
- Die Branche bildet im November 2009 im Rahmen des AK-TK eine „Arbeitsgruppe Schnittstellendefinition“ für diesen Zweck
- Als Ergebnis wird bereits im Februar die EPO20 den Ministerien vorgestellt

### Gesetzlicher Unterbau im Entwurf zur TKG-Novelle:

- § 94 Abs.4 TKG schlägt CSV File und Übermittlung durch verschlüsselte E-Mail (S/MIME-Standard) vor → schnellste Lösung unter Zeitdruck, verhindert jedenfalls direkten Zugang der Behörden zu den Systemen der Anbieter
- Festgelegt wird, dass es ein „push“ aus Sicht des Anbieters sein muss
- Verordnungsermächtigung in § 94 Abs. 4 TKG ist beschränkt auf die Festlegung der Syntax und Datenfelder des CSV File
- Protokollierungsvorschriften in § 102c TKG



Ludwig Boltzmann Institut für Menschenrechte (BIM)

## Studie des BIM: Entwurf einer Datensicherheits- Verordnung TKG (DSVO-TKG)

- **Nach dem Urteil des dt Bundesverfassungsgerichts (März 2010)**
  - das BIM schlägt dem BMVIT ein Konzept zur Umsetzung einer Datensicherheitsverordnung samt Schnittstellendefinition vor – auch auf TKG-Ebene soll nachgebessert werden
  - Ausserdem finden 3 Gesprächsrunden mit Vertretern von „geschützten Berufen“ (Ärzte, Rechtsanwälte, Notare, Journalisten, etc) statt → der Vorschlag einer Clearingstelle mit „Whitelist“ wird diskutiert – das BIM rät davon dringend ab
  - Daraus entsteht aber die Idee, zwar eine zentrale Drehscheibe für den Datenaustausch zu verwenden – allerdings „blind“ gegenüber den Inhalten!
- **Das BIM stellt sein Konzept vor und entwickelt es weiter in Diskussion mit**
  - Der Arbeitsgruppe Schnittstellendefinition des AK-TK
  - Sämtlichen Stakeholdern im Rahmen von insgesamt 6 Round Tables (BM.I, BMJ, BMVIT, BKA / BKA-VD, DSK, BMF, BRZ, Vertreter Internet- und Telekom- Wirtschaft, TU Wien, BIM)



Ludwig Boltzmann Institut für Menschenrechte (BIM)

## Hauptfrage: Wie soll die Kommunikation zwischen Anfrage- und Abfrageberechtigten ausschauen?

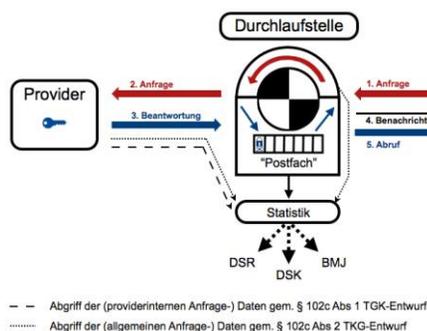
Verschiedene Möglichkeiten wurden diskutiert:

- Austausch via E-Mail (S/MIME) nach dem ursprünglichen Ansatz des BIM-Entwurf
- Konzept der Durchlaufstelle (DLS)
- ➔ DLS-Konzept auf Grund organisatorischer Vorteile von den Beteiligten letztlich vorgezogen



Ludwig Boltzmann Institut für Menschenrechte (BIM)

## Funktionsweise der DLS



- DLS fungiert als „Postfach“
- Anfrage und Datenübermittlung sind verschlüsselt
- Protokollierung und Erstellung einer Statistik durch die DLS



Ludwig Boltzmann Institut für Menschenrechte (BIM)

## Grundzüge des BIM-Entwurfs zur DSVO-TKG

- Übermittlung der Daten als CSV-File via DLS
- Strenge Unterscheidung von Betriebs- und Vorratsdaten
- Revisions sichere Protokollierung und Vier-Augen-Prinzip bei Zugriffen auf Vorratsdaten
- Optional möglich sind Stammdatenauskünfte über die DLS
- DLS nimmt Protokollierung vor, die keine personenbezogenen Daten enthält
- DLS erzeugt automatische Statistik
- Sichere Anbindung aller Beteiligten unter Nutzung des Portalverbunds



Ludwig Boltzmann Institut für Menschenrechte (BIM)

## Kritik an der endgültigen DSVO

Die Datensicherheitsverordnung gem. §§ 94 (4) und 102c TKG wurde schließlich am 6.12.2011 erlassen. Im wesentlichen entspricht diese dem Begutachtungsentwurf. Kritik ist aber zu üben:

- Streichung der vorgesehenen Klarstellung, dass vorab zulässige mündliche Anfragen nach SPG bei „Gefahr im Verzug“ über die DLS nachzureichen sind.
- Protokollierungspflichten wurden verwässert, wo eigentlich schon Klarheit bestand: zB Zugriff auf Vorratsdaten nach SPG Anfragen
- Durch Änderung der Protokollierungsvorschriften besteht nun auch die Gefahr, dass die Statistik für die EU-Kommission verfälscht wird

**Abschließend:**



Die DLS Umsetzung und die DSVO sind dennoch sehr zu begrüßen und bringen einen nach dem bisherigen Vergleich europaweit unvergleichbaren Datenschutz-Standard

Ludwig Boltzmann Institut für Menschenrechte (BIM)

Ludwig Boltzmann Institut für Menschenrechte (BIM)



Danke für Ihre  
Aufmerksamkeit!



Ein Institut der  
Ludwig Boltzmann Gesellschaft