

# Access to E-Evidence - Cost Reimbursement, Workflow & Challenges for ISPs

**Dr. Maximilian Schubert LL.M**

Vice President, Chair Cybersecurity Committee, EuroISPA  
General Secretary, ISPA Austria

**EC-Round Table, DG HOME, Rue du Luxembourg 46, 02.05.2017**

# EuroISPA – The voice of the ISPs in Europe

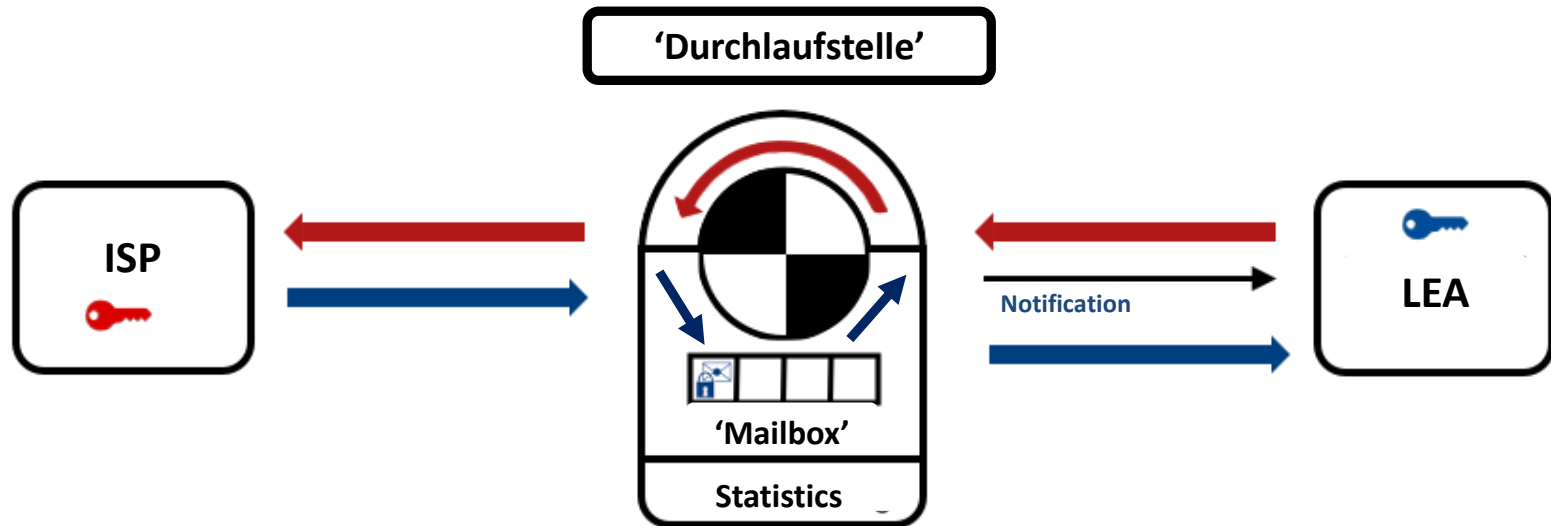
- Established in **1997**
- The world's largest association of Internet Services Providers (ISPs), representing over **2.500 ISPs** across the EU and EFTA countries
- Representing many SME-ISPs
- Reflects the views of ISPs of all sizes from across its member base



# **,Request for information` ≠ ,Lawful interception`**

- **Lawful interception requests**  
refer to future surveillance of a user's communication
  - Includes communication content
  - Permitted only for the prosecution of certain crimes
  - Call Content and Interception related data (IRI) are transferred via high secure interfaces to SPOC of national LEA
- **Requests for information**  
refer to access to data retained by ISPs
  - Contract data, traffic data (particularly IP-addresses)
  - Formal procedural requirements
  - Secure data transfer methods (DLS)

# Austrian Example for safe transfer of data between LE and ISPs - 'DLS'



# Workflow of the ISP (<- inbound)

- **Notification** about new „data providing“ request
- **Authentication** to the secure data environment (DLS)
- **Secure and encrypted transfer** from the secure data environment to the ISP
- **Decryption** and **verification** of received data
- Secure and encrypted **documentation of the request**

# Workflow of the ISP (- internal - 1)

- **Formal review** of the request  
(i.e. legitimization of requesting authority, formal criteria)
- **Contextual review** of the request  
(i.e. target, type of requested information, duration, date & time)
- **Legal review** of the request
- **Contact** with requesting or executing **authorities** (judicial or executive) to **clarify ambiguities** (fax, typos), if necessary
- **Documentation** of such contact

# Workflow of the ISP (- internal - 2)

- **Formal intern processing** of the request  
(i.e. documentation of the requested data, is the target a customer, etc.)
- **Internal data process** based on the request (i.e. data collection)
- **Verification of processed data** based on formal criteria  
(i.e. target, duration, date, time, typos, data set complete, etc.)
- **Documentation** of data gathering/process
- **Data conversion** to match national data standards

# Workflow of the ISP (-> outbound)

- **Authentication** to the secure data environment (DLS)
- Secure and encrypted **transfer** to the DLS
- **Documentation** of transfer
- Preparation of **cost reimbursement** request & following **review**
- Publication of yearly **transparency report**



# Need for cost reimbursement

- ISP are willing to co-operate with LE. Law Enforcement however is a **public/ official duty**, ISPs can not be burdened with covering these expenses; Austrian Const. Court- VfGH, G37/02, 27.02.2003
- **Cost reimbursement (OPEX, CAPEX) is foreseen** by most Member States.
- Application of the principle of **proportionality**.
- Internal workflow requires **personnel expenses** between minutes and hours, depending on the size of the ISP and frequency of such requests.
- **Maintenance** of the **technical infrastructure** & continuous **training of personnel** causes further expenses

# Current challenges

- **'perception dilemma'**
  - LE claim: Slow processing of requests & unwillingness
  - ISP claim: Low quality of requests & pressure by members of LE and judiciary who are not familiar with procedure (*'life ain't CSI'*)
- Need for specially trained personnel on both sides, *'SPOCs' vs 'deputy sheriffs'*
- Lacking use of **templates** & **official form**
- **Legal review**: complex legal background & uncertainties, (please see for example ISPA table for data requests – next slide)

# Challenge of Legal Review – Overview

## Beauskunftung - Übersicht

Rechtsgrundlage	Grundnorm (TKG)	Auskunft über	Anfrage-Art	DLS-Pflicht (Anfrage)	DLS-Pflicht (Antwort)	Anfragegeber, Stelle	Anfragegrund	"Begründung" (gegenüber NB)
<b>Sicherheitspolizeigesetz (SPG)</b>								
§ 53 Abs 3a Z 1 SPG	§ 90 Abs 7	Stammdaten <sup>(1)</sup>	schriftlich	(vorzugsweise) wenn optiert	ja, wenn optiert	Polizei <sup>(1)</sup>	SPG	nein
		Stammdaten <sup>(2)</sup>	schriftlich	nein	nein	Polizei <sup>(1)</sup>	SPG	nein
		Stammdaten <sup>(3)</sup>	(vorläufig)mündl. (Nenn. §907 TKG)	nein	nein	Polizei <sup>(1)</sup>	SPG - dringender Fall	nein - Nachrechnung
§ 53 Abs 3a Z 2 SPG	§ 99 Abs 5 Z 4	IP-Adressen Bekannngabe	schriftlich	ja	ja	Polizei	Gefahrenabwehr / EAH / krimin. Vlg.	nicht ausdrücklich vorgesehen
		IP-Adressen Bekannngabe	schriftlich	nein (bei GV)	nein	Polizei	Gefahrenabwehr / EAH / krimin. Vlg.	nicht ausdrücklich vorgesehen
§ 53 Abs 3a Z 3 SPG	§ 99 Abs 5 Z 4	Stammdaten zu IP-Adresse	schriftlich	ja	ja	Polizei	Gefahrenabwehr / EAH / krimin. Vlg.	nicht ausdrücklich vorgesehen
		Stammdaten zu IP-Adresse	schriftlich	nein (bei GV)	nein	Polizei	Gefahrenabwehr / EAH / krimin. Vlg.	nicht ausdrücklich vorgesehen
§ 53 Abs 3a Z 4 SPG	§ 99 Abs 5 Z 3	passive Rufdaten	schriftlich	ja	ja	Polizei	Gefahrenabwehr / EAH	nicht ausdrücklich vorgesehen
		passive Rufdaten	schriftlich	nein (bei GV)	nein	Polizei	Gefahrenabwehr / EAH	nicht ausdrücklich vorgesehen
§ 53 Abs 3b SPG	§ 99 Abs 5 Z 3	IMEI, Standort	schriftlich	nein (da immer GV - "gegenwärtig")	nein	Polizei	Gefahrenabwehr / EAH	ja
		IMEI, Standort	mündlich	nein (da immer GV - "gegenwärtig")	nein	Polizei	Gefahrenabwehr / EAH	ja - Nachrechnung
<b>Strafprozessordnung (StPO)</b>								
§ 76a Abs 1 StPO	§ 90 Abs 7	Stammdaten	schriftlich	(vorzugsweise) wenn optiert	ja, wenn optiert	Gefichte, SA, Polizei	Strafz	nein
		Stammdaten	schriftlich	nein	nein	Gefichte, SA, Polizei	Strafz	nein
		Stammdaten	(vorläufig)mündl. (Nenn. §907 TKG)	nein	nein	Gefichte, SA, Polizei	Strafz - dringender Fall	nein - Nachrechnung
§ 76a Abs 2 Z 1, Z 4; Fall StPO	§ 99 Abs 5 Z 2	IP-Adresse, E-Mail & IP-Adr. des Absenders	schriftlich	ja (auch bei GV)	ja	Geficht, SA	Strafz (Anordnung der SA)	nein (Anordnung)
		E-Mail-Adresse	schriftlich	nein (optional)	nein (optional)	Geficht, SA	Strafz (Anordnung der SA)	nein (Anordnung)
§ 154 Z 2 / 155 Abs 2 StPO	§ 99 Abs 5 Z 1	Verkehrsdaten	schriftlich	ja	ja	Gefichte, SA, Polizei	Strafz (gerichtlich bewilligte Anordnung der SA)	nein (Anordnung)
		Zugangsdaten (eingeschränkt auf IMSI, IMEI) <sup>(2)</sup>	schriftlich	ja	ja	Gefichte, SA, Polizei	Strafz (gerichtlich bewilligte Anordnung der SA)	nein (Anordnung)
		Standortdaten (historisch / "backoffice")	schriftlich	ja	ja	Gefichte, SA, Polizei	Strafz (gerichtlich bewilligte Anordnung der SA)	nein (Anordnung)
		Standortdaten (aktuelle Peilung)	schriftlich	nein	nein	Gefichte, SA, Polizei	Strafz (gerichtlich bewilligte Anordnung der SA)	nein (Anordnung)
<b>Telekommunikationsgesetz (TKG)</b>								
§ 99 Abs 6 TKG	-	Stammdaten	schriftlich	nein	nein	Verwaltungsbehörden	Verwaltungsüberhebung	ja
§ 99 Abs 7 TKG	-	Stammdaten	schriftlich	(vorzugsweise) wenn optiert	ja, wenn optiert	Gefichte, SA, Polizei	Strafz	nein
		Stammdaten	schriftlich	nein	nein	Gefichte, SA, Polizei	Strafz	nein
		Stammdaten	(vorläufig)mündl.	nein	nein	Gefichte, SA, Polizei	Strafz - dringender Fall	nein, aber Nachrechnung
§ 99 Abs 1 TKG	-	Stammdaten	schriftlich	nein	nein	Nutzerkenn-Betreiber	Notfall	ja (da Anfrage durch 3. Person)
		Stammdaten	schriftlich	nein	nein	Nutzerkenn-Betreiber	Notfall	ja - Nachrechnung
		Standortdaten (Benachrichtigung des Betroffenen)	schriftlich	nein	nein	Nutzerkenn-Betreiber	Notfall	ja (da Anfrage durch 3. Person)
		Standortdaten (Benachrichtigung des Betroffenen)	mündlich	nein	nein	Nutzerkenn-Betreiber	Notfall	ja - Nachrechnung
§ 98 Abs 3 TKG (Schlüssel-NRT)	-	Stammdaten	schriftlich	nein (Schlüssel-NRT)	nein (Schlüssel-NRT)	Nutzerkenn-Betreiber	Notfall	nein (da Gesuchter direkt)
		Stammdaten	mündlich	nein (Schlüssel-NRT)	nein (Schlüssel-NRT)	Nutzerkenn-Betreiber	Notfall	nein (da Gesuchter direkt)
		Standortdaten (Benachrichtigung des Betroffenen)	schriftlich ("nummernbar")	nein (Schlüssel-NRT)	nein (Schlüssel-NRT)	Nutzerkenn-Betreiber	Notfall	nein (da Gesuchter direkt)
		Standortdaten (Benachrichtigung des Betroffenen)	mündlich ("nummernbar")	nein (Schlüssel-NRT)	nein (Schlüssel-NRT)	Nutzerkenn-Betreiber	Notfall	nein (da Gesuchter direkt)
<b>DIVERSES</b>								
<b>Rechtsgrundlage</b>								
§ 99 Abs 3 FinStBG	-	Stammdaten (erweiterte Pflichten)	schriftlich	nein	nein	Finanzstrafbehörde	Finanzstrafverfahren	nein
§ 99 Abs 3a FinStBG	ja/nein	Verkehrsdaten (IP-Adresse, Name & Anschrift zu IP-Adresse)	schriftlich	ja	ja	Finanzstrafbehörde	Finanzstrafverfahren (Anordnung des Senatvorsitzenden)	ja
§ 11 Abs 12 4 PSStG	§ 90 Abs 7	Stammdaten	schriftlich	(vorzugsweise) wenn optiert	ja, wenn optiert	BVT, LV	PSStG, Ermächtigung des DSB bei BMI	nein
		Stammdaten	schriftlich	nein	nein	BVT, LV	PSStG, Ermächtigung des DSB bei BMI	nein
		Stammdaten	(vorläufig)mündl. (Nenn. §907 TKG)	nein	nein	BVT, LV	PSStG, Ermächtigung des DSB bei BMI	nein
§ 11 Abs 12 5 PSStG	§ 99 Abs 5 Z 3	IP-Adressen Bekannngabe	schriftlich	ja	ja	BVT, LV	PSStG, Ermächtigung des DSB bei BMI	nein
		IP-Adressen Bekannngabe	schriftlich	nein (bei GV)	nein	BVT, LV	PSStG, Ermächtigung des DSB bei BMI	nein
		IMEI, Standort	schriftlich	nein (da immer GV - "gegenwärtig")	nein	BVT, LV	PSStG, Ermächtigung des DSB bei BMI	nein
		IMEI, Standort	mündlich	nein (da immer GV - "gegenwärtig")	nein	BVT, LV	PSStG, Ermächtigung des DSB bei BMI	nein
§ 11 Abs 12 7 PSStG	§ 99 Abs 5 Z 5	Verkehrsdaten, Standort, Zugangsdaten	schriftlich	ja	ja	BVT, LV	Strafz mit mehr als 1 J. FS; Ermächtigung des	Ermächtigung des Rechtschutzsenats ist anzufragen
§ 148 BAO	-	(je Stammdaten (erweiterte Pflichten))	schriftlich	nein	nein	Abgabenbehörde	Erhebung von Abgaben	nein
§ 48b Abs 3 BörseG	ja/nein	Verkehrsdaten, Standortdaten, Zugangsdaten, Stammdaten	schriftlich	ja	ja	Finanzmarktaufsicht	Verwaltungsüberhebung	Gerichtlich bewilligte Anordnung der FMA
§ 14b UWG	-	Name, Anschrift anhand Rufnummer	schriftlich	nein	nein	HR Schutzverband	Verdacht unläutlicher Geschäftspraxis	ja
§ 22 Abs 2a MiBG	-	Stammdaten zu Rufnummer	schriftlich	nein	nein	militär, Organe	schlichter Dienst, Aufklärung/Abwehr	nein

Hinweis: Statische festgelegte zugewiesene IP-Adressen werden als Stammdaten behandelt. Dynamische IP-Adressen werden als Zugangsdaten behandelt.

<sup>(1)</sup> Gerichte, SA und Kriminalpolizei; Auskunft über Stammdaten (§ 90 (7) TKG); Sicherheitsbehörden; nur Name, Anschrft, Teilnehmernummer (§ 53 (3a) Z 1 SPG)

<sup>(2)</sup> Die Beauskunftung von dynamische IP-Adressen sowie die in § 76a Abs. 2 StPO angeführten Email-Daten darf ab 01.04.12 nur nach Anordnung des SA gem § 102 StPO erfolgen.

Hinweis: Durch Mausklick auf die Rechtsgrundlage der Anfragen (Spalte A) oder der korrespondierende Norm im TKG (Spalten B) gelangen Sie zu der jeweiligen Bestimmung im Rechtsinformationssystem (RIS).

# Challenges related to requests by foreign authorities

- Difficulties concerning **verification** of requesting authority, **plausibility of request & integrity**
  - Legal review hampered by **lack of expertise in foreign law**
- Difficulties in **communication** with foreign authorities (language barrier)
- ISP is bound towards users to comply with national law
  - Risk of **circumvention of national rules** by filing a request at a foreign authority
  - **'double criminality'** requirement

# Thank You!



## **EuroISPA**

European Internet Services Providers Association  
Rue du Commerce 124/5 - 1000 Brussels  
T: +32 (0)2 550 41 22  
[www.euroispa.org](http://www.euroispa.org)

EU Transparency Register No. 54437813115-56

Dr. Maximilian Schubert, General Secretary  
**ISPA - Internet Service Providers Austria**  
Währinger Straße 3/18 - 1090 Vienna  
T: +43 1 409 55 76

Email [maximilian.schubert@ispa.at](mailto:maximilian.schubert@ispa.at)  
Web [www.ispa.at](http://www.ispa.at)

EU Transparency Register No. 56028372438-43