„Europäisches Strafrecht nach der österreichischen Ratspräsidentschaft“

E-Evidence Verordnungsvorschlag: Die Sicht der Diensteanbieter

Dr. Maximilian Schubert, LL.M.

07.03.2019, Wirtschaftsuniversität Wien

ispa Internet Service Providers Austria

Agenda

Über ISPA

Provider-interne Ablauf einer Beauskunftung

Herausforderungen im Kontext der Kooperation ISP – LEAs

E-Evidence-Verordnungsvorschlag

Vorschlag gg. die Verbreiterung von terroristischen Online-Inhalten

ispa Internet Service Providers Austria

Die ISPA vertritt die Internetwirtschaft

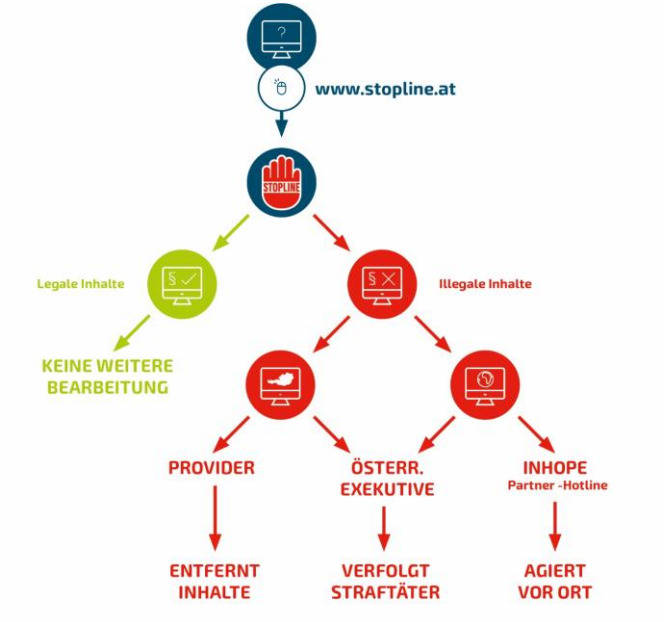
- **Gegründet 1997**
- **215 Mitglieder aus den Bereichen**
  - **Access**
  - **Hosting**
  - **Content & Services**
- **Zwei Drittel weniger als 25 Mitarbeiterinnen oder Mitarbeiter**

www.stopline.at

Meldestelle gegen
Sexuelle Missbrauchsdarstellungen Minderjähriger & nationalsozialistische Wiederbetätigung im Internet

ispa Internet Service Providers Austria

Stopline.at



www.stopline.at

Meldestelle gegen
Sexuelle Missbrauchsdarstellungen Minderjähriger & nationalsozialistische Wiederbetätigung im Internet

INTERNATIONAL ASSOCIATION OF INTERNET HOTLINES
INHOPE

www.inhope.org
Internationale Netzwerk von Beschwerdestellen zur Bekämpfung illegaler Inhalte

ispa Internet Service Providers Austria

Sonstige Aktivitäten

EuroISPA ist der weltweit größte Provider-Dachverband, der die Interessen von über 2.500 ISPs vertritt

Roundtable on cross-border access to e- evidence and the role of encryption in criminal investigations

EUIPO
AMT DER EUROPÄISCHEN UNION FÜR GEISTIGES EIGENTUM

Amt der Europäischen Union für geistiges Eigentum

Saferinternet.at
Das Internet sicher nutzen!

Awareness-Center des Safer Internet Konsortium

NO HATE SPEECH MOVEMENT

Nationales "No Hate Speech" Komitee

ispa Internet Service Providers Austria

ISPA Informationsmaterial

Kostenlos downloaden und bestellen:
www.ispa.at/broschuren

ispa Internet Service Providers Austria

Der Online-Zoo

ispa Internet Service Providers Austria

Agenda

Über ISPA

Provider-interner Ablauf einer Beauskunftung

Herausforderungen im Kontext der Kooperation ISP – LEAs

E-Evidence-Verordnungsvorschlag

Vorschlag gg. die Verbreiterung von terroristischen Online-Inhalten

Beauskunftung ≠ Überwachung

- **Überwachung**: bezieht sich auf die Überwachung der zukünftigen Kommunikation eines Benutzers
  - Enthält Inhaltsdaten
  - Nur für die Verfolgung bestimmter Straftaten erlaubt
  - Anrufinhalt und abhörbezogene Daten werden über hochsichere Schnittstellen an SPOC der nationalen LEA übermittelt

- **Beauskunftungsanfrage**: bezieht sich auf den Zugriff auf Daten, die von ISPs gespeichert werden
  - Stammdaten, Verkehrsdaten (insbesondere IP-Adressen)
  - Formale Verfahrensanforderungen
  - Sichere Datenübertragungsmethoden (DLS)

Arbeitsschritte (<- Eingang)

- Anfrage zur **Datenbeauskunftung**
- **Authentifizierung** (DLS)
- Sichere und **verschlüsselte Übertragung** zum ISP
- **Entschlüsselung** und **Verifizierung** der empfangenen Daten
- Sichere und **verschlüsselte Dokumentation** der Anfrage

Arbeitsschritte (- intern - 1)

- **Formale Überprüfung der Anfrage**
  (z.B. Legitimität der anfragenden Stelle, formale Kriterien)
- **Inhaltliche Überprüfung**
  (z.B. Betroffener, Art der angefragten Informationen, technische Kriterien des zu überwachenden Targets, Zeitraum, Rechtsgrundlage)
- **Rechtliche Überprüfung**
- **Gegebenenfalls Rückfrage bei der anfragenden Stelle** (Gericht StA oder Behörde) sofern notwendig - § 1 Abs. 2 ÜKVO
- **Dokumentation** von derartigen Rückfragen

Arbeitsschritte (- intern - 2)

- **Formal interne Arbeitsabläufe** bei der Beauskunftung (z. B. Dokumentation der angeforderten Daten, ist das Ziel ein Kunde usw.)
- **Interne Datenanalyse**
  (Datenbanken abfragen, Daten verknüpfen wenn aus unterschiedlichen Quellen)
- Daten zum Transport in **richtiges Format** aufbereiten

Arbeitsschritte (-> Ausgang)

- **Authentifizierung** in der Durchlaufstelle
- Sichere und **verschlüsselte Übertragung** (TKG-DSVO-konform)
- **Dokumentierung** der Beauskuftung
- Vorbereitung der **Kostenerstattungsanforderung** und anschließende Überprüfung
- Veröffentlichung des jährlichen **Transparenzberichts**

Agenda

Über ISPA

Provider-interner Ablauf einer Beauskunftung

Herausforderungen im Kontext der Kooperation ISP – LEAs

E-Evidence-Verordnungsvorschlag

Vorschlag gg. die Verbreiterung von terroristischen Online-Inhalten

Aktuelle Herausforderungen

„Das Wahrnehmungsdilemma"

- LEA-Sicht: Langsame Bearbeitung von Anfragen und Unwilligkeit der Betreiber
- ISP-Sicht: Unterschiedliche Qualität der Anfragen und Druck von Vertretern der LEA sowie der Justiz, die mit dem Ablauf nicht vertraut sind („***Life ain't CSI***")

- Bedarf an speziell geschultem Personal auf beiden Seiten, **„ SPOCs" vs. „deputy Sheriffs"**
- **Vertrauensbildung** zwischen ISPs und Behörden
- Strikte Verwendung von **Vorlagen** und **offiziellem Formular**
- **Rechtliche Überprüfung**: Komplexe rechtliche Hintergründe und Unsicherheiten

ispa Internet Service Providers Austria

ISPA Beauskunftungsübersicht

Beauskunftung - Übersicht

Rechtsgrundlage	Grundnorm (TKG)	Auskunft über	Anfrage- Art	DLS-Pflicht (Anfrage)	DLS-Pflicht (Antwort)	Anfrageber. Stelle	Anfragegrund	"Begründung" (gegenüber NB)
Sicherheitspolizeigesetz (SPG)								
§ 53 Abs 3a Z 1 SPG	§ 90 Abs 7	Stammdaten[1)]	schriftlich	(vorzugsweise) wenn optiert	ja, wenn optiert	Polizei[1)]	SPG	nein
		Stammdaten[1)]	schriftlich	nein	nein	Polizei[1)]	SPG	nein
		Stammdaten[1)]	(vorläufig) mündl. (Verw. § 90/7 TKG)	nein	nein	Polizei[1)]	SPG - dringender Fall	nein - Nachreichung
§ 53 Abs 3a Z 2 SPG	§ 99 Abs 5 Z 4	IP-Adressen-Bekanntgabe	schriftlich	ja	ja	Polizei	Gefahrenabwehr / EAH / krimin. Vbg	nicht ausdrücklich vorgesehen
		IP-Adressen-Bekanntgabe	schriftlich	nein (bei GiV)	nein	Polizei	Gefahrenabwehr / EAH / krimin. Vbg	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. Vbg	nicht ausdrücklich vorgesehen
		Stammdaten zu IP-Adresse	schriftlich	nein (bei GiV)	nein	Polizei	Gefahrenabwehr / EAH / krimin. Vbg	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 GiV)	nein	Polizei	Gefahrenabwehr / EAH	nicht ausdrücklich vorgesehen
§ 53 Abs 3b SPG	§ 99 Abs 5 Z 3	IMSI, Standort	schriftlich	nein (da immer GiV - "gegenwärtig")	nein	Polizei	Gefahrenabwehr / EAH	ja
		IMSI, Standort	mündlich	nein (da immer GiV - "gegenwärtig")	nein	Polizei	Gefahrenabwehr / EAH	ja - Nachreichung!
Strafprozessordnung (StPO)								
§ 76a Abs 1 StPO	§ 90 Abs 7	Stammdaten	schriftlich	(vorzugsweise) wenn optiert	ja, wenn optiert	Gerichte, StA, Polizei	Strafsat	nein
		Stammdaten	schriftlich	nein	nein	Gerichte, StA, Polizei	Strafsat	nein
		Stammdaten	(vorläufig) mündl. (Verw. § 90/7 TKG)	nein	nein	Gerichte, StA, Polizei	Strafsat - dringender Fall	nein - Nachreichung
§ 76a Abs 2 Z 1, Z 4 2. Fall StPO	§ 99 Abs 5 Z 2	IP-Adresse, E-Mail & IP-Adr. des Absenders	schriftlich	ja (auch bei GiV)	ja	Gericht, StA	Strafsat (Anordnung der StA)	nein (Anordnung)
§ 76a Abs 2 Z 2 - 3 StPO		E-Mail-Adresse	schriftlich	nein (optional)	nein (optional)	Gericht, StA	Strafsat (Anordnung der StA)	nein (Anordnung)
§§ 134 Z 2 / 135 Abs 2 StPO	§ 99 Abs 5 Z 1	Verkehrsdaten	schriftlich	ja	ja	Gerichte, StA, Polizei	Strafsat (gerichtlich bewilligte Anordnung der StA)	nein (Anordnung)
		Zugangsdaten (eingeschränkt auf IMSI, IMEI)[2)]	schriftlich	ja	ja	Gerichte, StA, Polizei	Strafsat (gerichtlich bewilligte Anordnung der StA)	nein (Anordnung)
		Standortdaten (historisch / fortlaufend)	schriftlich	ja	ja	Gerichte, StA, Polizei	Strafsat (gerichtlich bewilligte Anordnung der StA)	nein (Anordnung)
		Standortdaten (aktuelle Peilung)	schriftlich	nein	nein	Gerichte, StA, Polizei	Strafsat (gerichtlich bewilligte Anordnung der StA)	nein (Anordnung)
Telekommunikationsgesetz (TKG)								
§ 90 Abs 6 TKG	-	Stammdaten	schriftlich	nein	nein	Verwaltungsbehörden	Verwaltungsübertretung	ja
§ 90 Abs 7 TKG	-	Stammdaten	schriftlich	(vorzugsweise) wenn optiert	ja, wenn optiert	Gerichte, StA, Polizei	Strafsat	nein
		Stammdaten	schriftlich	nein	nein	Gerichte, StA, Polizei	Strafsat	nein
		Stammdaten	(vorläufig) mündl.	nein	nein	Gerichte, StA, Polizei	Strafsat - dringender Fall	nein, aber Nachreichung
§ 98 Abs 1 TKG	-	Stammdaten	schriftlich	nein	nein	Notrufdienst-Betreiber	Notfall	ja (da Anfrage durch 3. Person)
		Stammdaten	mündlich	nein	nein	Notrufdienst-Betreiber	Notfall	ja - Nachreichung!
		Standortdaten (Benachrichtigung des Betroffenen)	schriftlich	nein	nein	Notrufdienst-Betreiber	Notfall	ja (da Anfrage durch 3. Person)
		Standortdaten (Benachrichtigung des Betroffenen)	mündlich	nein	nein	Notrufdienst-Betreiber	Notfall	ja - Nachreichung!
§ 98 Abs 3 TKG (Schnittst.NRT)	-	Stammdaten	schriftlich	nein (Schnittst.NRT)	nein (Schnittst.NRT)	Notrufdienst-Betreiber	Notfall	nein (da Gesuchter direkt)
		Stammdaten	mündlich	nein (Schnittst.NRT)	nein (Schnittst.NRT)	Notrufdienst-Betreiber	Notfall	nein (da Gesuchter direkt)
		Standortdaten (Benachrichtigung des Betroffenen)	schriftlich ("unmittelbar")	nein (Schnittst.NRT)	nein (Schnittst.NRT)	Notrufdienst-Betreiber	Notfall	nein (da Gesuchter direkt)
		Standortdaten (Benachrichtigung des Betroffenen)	mündlich ("unmittelbar")	nein (Schnittst.NRT)	nein (Schnittst.NRT)	Notrufdienst-Betreiber	Notfall	nein (da Gesuchter direkt)

DIVERSES								
Rechtsgrundlage		**Auskunft über**	**Anfrage - Art**	**DLS-Pflicht (Anfrage)**	**DLS-Pflicht (Antwort)**	**Anfrageber. Stelle**	**Anfragegrund**	**"Begründung" (gegenüber NB)**
§ 99 Abs 3 FinStrG	-	Stammdaten (erweitere Pflichten)	schriftlich	nein	nein	Finanzstrafbehörde	Finanzstrafverfahren	nein
§ 99 Abs 3a FinStrG	fehlt!!	Verkehrsdaten (IP-Adresse, Name & Anschrift zu IP-Adresse)	schriftlich	ja	ja	Finanzstrafbehörde	Finanzstrafverfahren (Anordnung des Senatsvorsitzenden	ja
§ 11 Abs 1 Z 5 PStSG	§ 90 Abs 7	Stammdaten	schriftlich	(vorzugsweise) wenn optiert	ja, wenn optiert	BVT, LV	PStSG, Ermächtigung des DSB bei BMI	nein
		Stammdaten	schriftlich	nein	nein	BVT, LV	PStSG, Ermächtigung des DSB bei BMI	nein
		Stammdaten	(vorläufig) mündl. (Verw. § 90/7 TKG)	nein	nein	BVT, LV	PStSG, Ermächtigung des DSB bei BMI	nein
§ 11 Abs 1 Z 5 PStSG	§ 99 Abs 5 Z 3	IP-Adressen-Bekanntgabe	schriftlich	ja	ja	BVT, LV	PStSG, Ermächtigung des DSB bei BMI	nein
		IP-Adressen-Bekanntgabe	schriftlich	nein (bei GiV)	nein	BVT, LV	PStSG, Ermächtigung des DSB bei BMI	nein
		IMSI, Standort	schriftlich	nein (da immer GiV - "gegenwärtig")	nein	BVT, LV	PStSG, Ermächtigung des DSB bei BMI	nein
		IMSI, Standort	mündlich	nein (da immer GiV - "gegenwärtig")	nein	BVT, LV	PStSG, Ermächtigung des DSB bei BMI	nein
§ 11 Abs 1 Z 7 PStSG	§ 99 Abs 5 Z 5	Verkehrsdaten, Standort, Zugangsdaten	schriftlich	ja	ja	BVT, LV	Straftat mit mehr als 1 J. FS; Ermächtigung des	Ermächtigung des Rechts-schutzsenats ist anzuführen
§ 143 BAO	-	ge Stammdaten (erweitere Pflichten)	schriftlich	nein	nein	Abgabenbehörde	Erhebung von Abgaben	nein
§ 48b Abs 3 BörseG	fehlt!!	Verkehrsdaten, Standortdaten, Zugangsdaten, Stammdaten	schriftlich	ja	ja	Finanzmarktaufsicht	Verwaltungsübertretung	Gerichtlich bewilligte Anordnung der FMA
§ 14a UWG	-	Name, Anschrift anhand Rufnummer	schriftlich	nein	nein	idR Schutzverband	Verdacht unlauterer Geschäftspraxis	ja
§ 22 Abs 2a MBG	-	Stammdaten zu Rufnummer	schriftlich	nein	nein	militär. Organe	nachrichtendienstl. Aufklärung/Abwehr	nein

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

[1)] Gerichte, StA und Kriminalpolizei: Auskunft über Stammdaten (§ 90 (7) TKG); Sicherheitsbehörden: nur Name, Anschrift, Teilnehmernummer (§ 53 (3a) Z 1 SPG)
[2)] 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 StA gem § 102 StPO erfolgen.

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

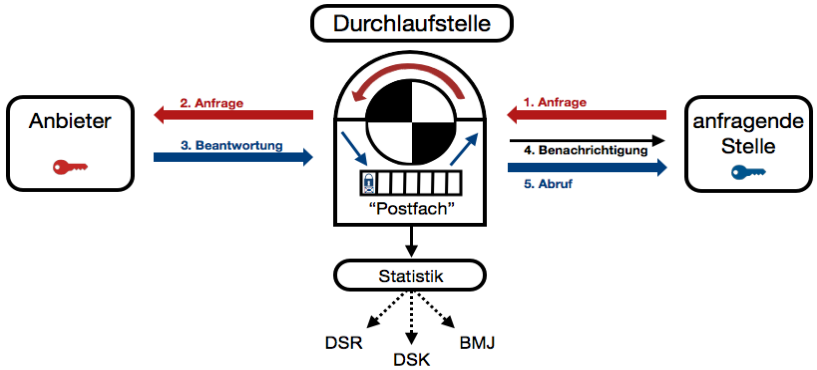
v.0.4.3., 15.09.2016

Die Stimme der Internetwirtschaft in Österreich

ispa Internet Service Providers Austria

Technische Herausforderungen

- **Schnelle, sichere und transparente** Datenübertragung
  - Unterschiedliche Systeme im Einsatz bei ISPs & LEA
  - Limitierte Ressourcen
  - ‘n x m’ Problematik (200+ ISPs, x Behörden)



Erfolgsraten bei Beauskunftungsanfragen (I)

Budapest Convention

	Requests for data directly sent to Apple, Facebook, Google, Microsoft, Twitter and Oath in 2017		
Parties and Observers (70 States)	Received	Disclosure	%
Albania	27	14	53%
Belgium	2 521	2 301	91%
Cabo Verde	40	20	50%
Croatia	196	166	85%
France	29 400	18 466	63%
Germany	35 596	20 172	57%
Mauritius	2	0	0%
Morocco	30	18	59%
Nigeria	7	5	71%
Portugal	3 569	2 394	67%
Senegal	2	0	0%
Turkey	8 618	4 739	55%
United Kingdom	31 954	23 073	72%
Total (excluding USA)	170 680	109 093	64%

Erfolgsraten bei Beauskunftungsanfragen (II)

- Die Erfolgsrate bei Beauskunftungsanfragen variiert sehr stark innerhalb der EU, abhängig von der Qualität der Anfragen
- Beauskunftete Daten aufgrund einer LEA Anfrage Jänner-Juli 2018:
  - **Facebook:** Niederlande **88%** Österreich **36%**
  - **Google:** Niederlande **64%** Österreich **51%**

Quellen: Transparency reports Google & FB

Notwendiger Kostenersatz

- ISPs sind bereit mit den LEA zusammenzuarbeiten. Die Strafverfolgung stellt jedoch eine **staatliche Aufgabe** dar. ISPs können nicht mit der Tragung dieser Kosten belastet werden. (VfGH, G37 / 02, 27.02.2003)
- Die meisten europäischen Staaten sehen **Kostenersatz (OPEX, CAPEX)** vor
- Grundsatz der **Verhältnismäßigkeit**, Beschränkung auf das Notwendigste
- Der interne Arbeitsablauf erfordert **Personalkosten**. Abhängig von der Größe des ISPs und der Häufigkeit solcher Anfragen kann es sich dabei um Minuten oder Stunden handeln
- Die **Wartung der technischen Infrastruktur** & die ständige **Personalschulung** verursachen weitere Kosten

Agenda

Über ISPA

Provider-interner Ablauf einer Beauskunftung

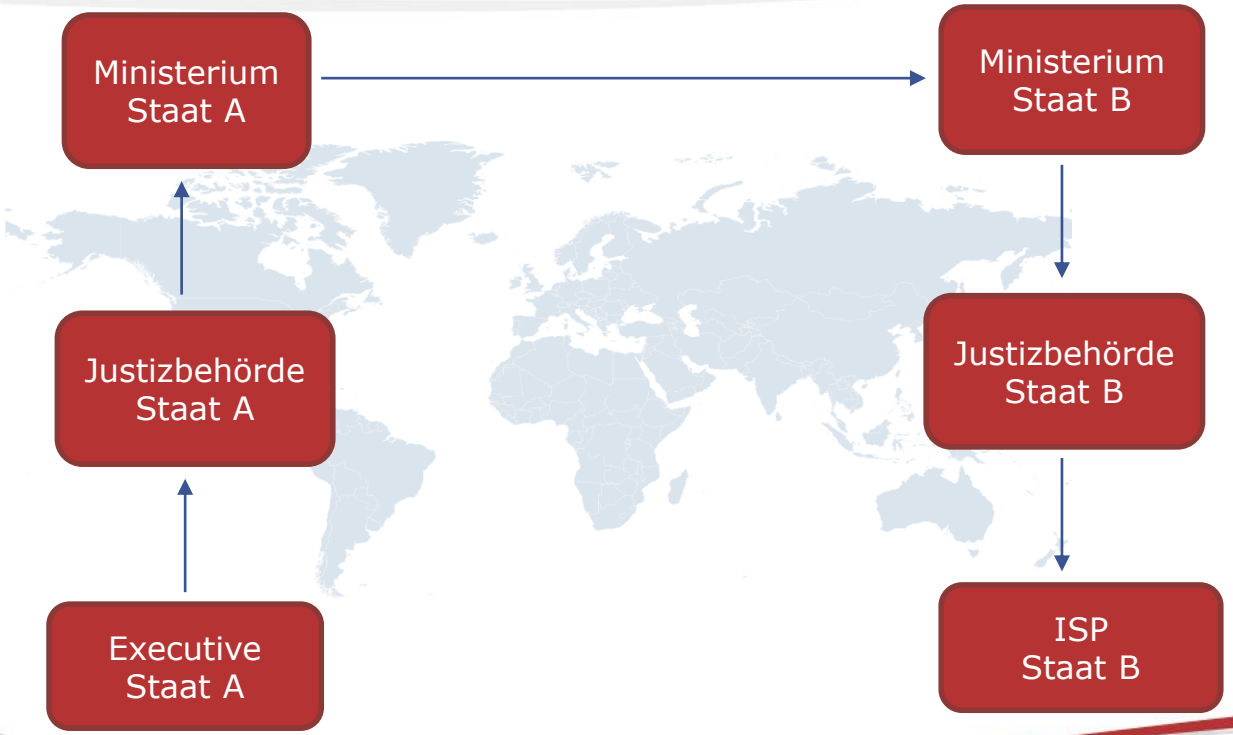
Herausforderungen im Kontext der Kooperation ISP – LEAs

E-Evidence-Verordnungsvorschlag

Vorschlag gg. die Verbreiterung von terroristischen Online-Inhalten

E-Evidence Verordnungsvorschlag

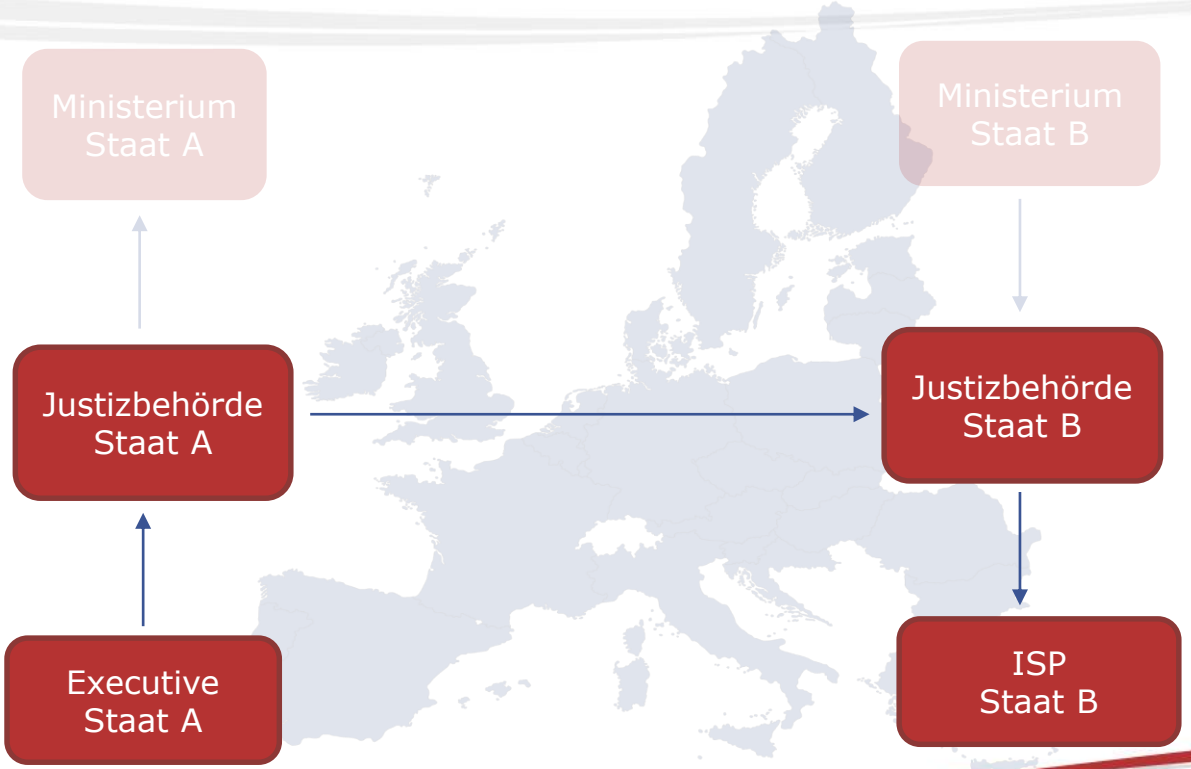
E-Evidence Verordnungsvorschlag



Das derzeitige MLAT Verfahren mit Drittländern

ispa Internet Service Providers Austria

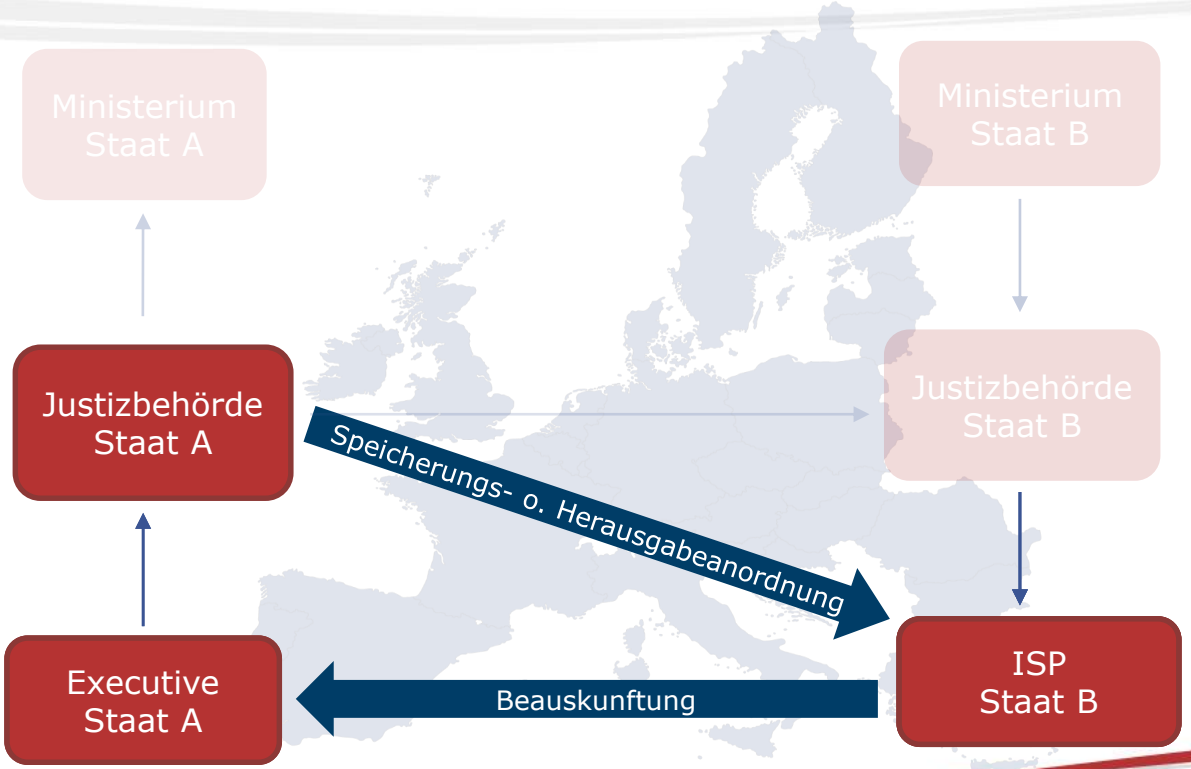
E-Evidence Verordnungsvorschlag



Amtshilfeverfahren in der EU

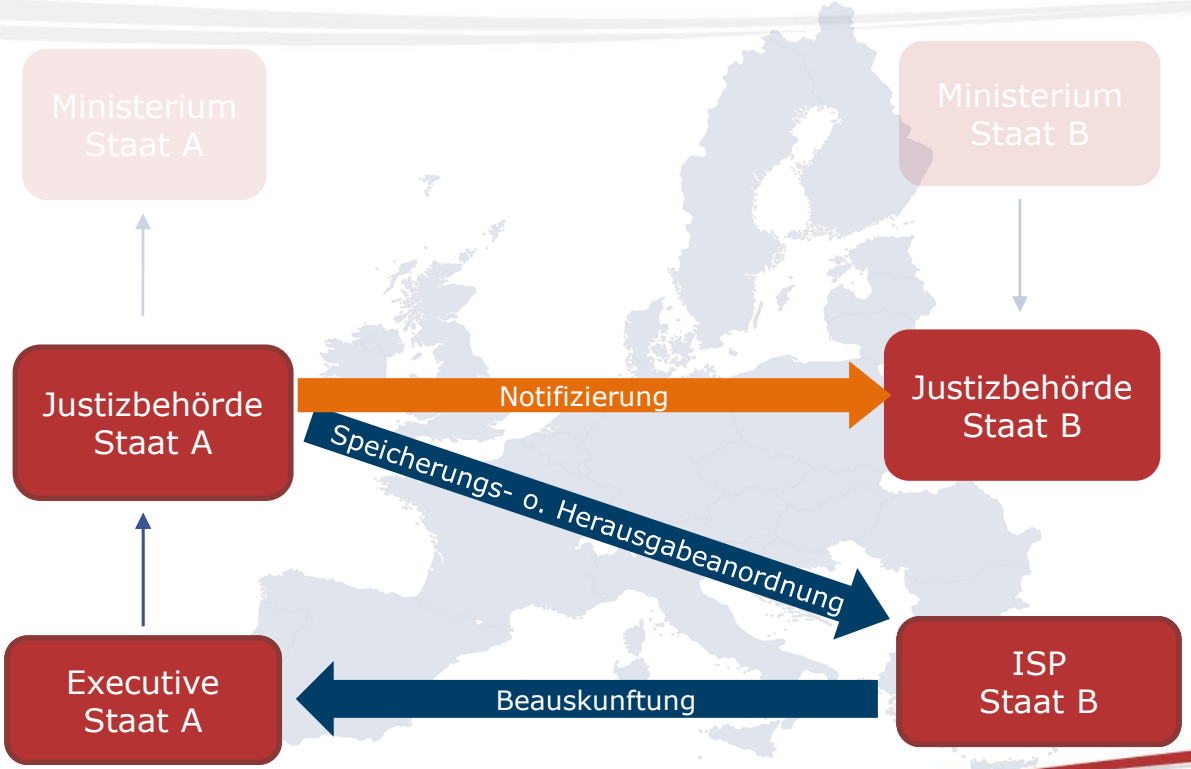
ispa Internet Service Providers Austria

E-Evidence Verordnungsvorschlag



E-Evidence Vorschlag

E-Evidence Verordnungsvorschlag

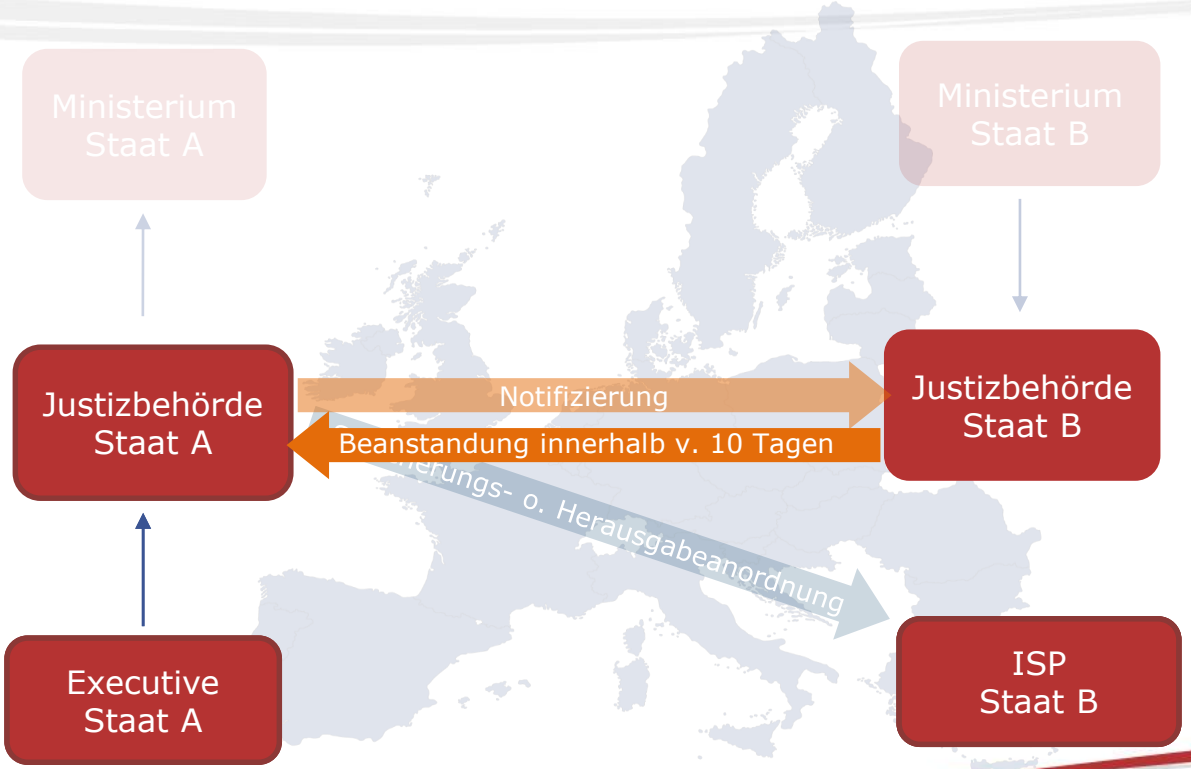


E-Evidence Vorschlag

Inhaltsdaten

ispa Internet Service Providers Austria

E-Evidence Verordnungsvorschlag



E-Evidence Vorschlag

Inhaltsdaten

ispa Internet Service Providers Austria

E-Evidence Verordnungsvorschlag Rechtsunsicherheit

- **Anordnungsschwelle**: signifikante Unterschiede zwischen den Mitgliedstaaten bei Straftaten mit dreijähriger Freiheitsstrafe
- **Doppelkriminalität** als Schlüsselfaktor für ISPs
- Unzureichende **Authentifizierung** von Anordnungen
  - ISPs sind nicht in der Lage die Echtheit des Stempels und der Unterschrift der einzelnen nationalen Justizbehörden zu verifizieren
- **Single Points of Contact (SPOC)** im vollstreckenden Staat würde den Kommunikationsablauf wesentlich verbessern

E-Evidence Verordnungsvorschlag
Mangel an Rechtsschutz & tech. Safeguards

- **Gerichtliche Kontrolle**: Nach der Rechtsprechung des EuGHs u EGMRs sollte der Zugang der Exekutive zu gespeicherten Daten von einem Gericht oder einer unabhängigen Verwaltungsbehörde überprüft werden (EuGH Tele2 Sverige, EGMR Benedik/Slowenien)
- **Verhältnismäßigkeit und Erforderlichkeit der Anordnung**: Die ISPs sollten über ausreichende Informationen verfügen, um ggf. Anordnungen anfechten zu können
- **Beteiligung der Behörden**: Auch entweder die zuständige Behörde im vollstreckenden Staat oder im Wohnsitzstaat des Betroffenen soll involviert werden
- **Sicherheit und die Integrität** der Datenübertragung

  Vorbehalte gegen ein Downgrade der bestehenden Standards zum Informationsaustausch z.B. durch Faxaussendungen

ispa Internet Service Providers Austria

E-Evidence Verordnungsvorschlag
Mangel an Rechtsschutz & tech. Safeguards

- **Gerichtliche Kontrolle:** Nach der Rechtsprechung des EuGHs u. EGMRs prüft der Zugriff der Exekutive zu gespeicherten Daten von einem Gericht oder einer unabhängigen Verwaltungsbehörde überprüft werden (EuGH Tele2 Sverige, EGMR Benedik/Slowenien)
- **Verhältnismäßigkeit und Erforderlichkeit der Anordnung:** Die Tats. sollten über ausreichende Informationen verfügen, um Art. Anordnungen entsprechen zu können
- **Beteiligung der Behörden.** Auch zuständige Behörde im vollstreckenden Staat oder im Wohnsitzstaat des Betroffenen soll involviert werden
- **Sicherheit und die Integrität der Datenübertragung**

  Vorkehrungen gegen den Einsatz der bestehenden Standards z.B. Informationssicherheit z.B. durch Verschlüsselungen

E-Evidence Verordnungsvorschlag
Offene Fragen im Kontext der Notifizierung

- **Benachrichtigung des Betroffenen**: Benachrichtigung über die Anordnung zur Herausgabe von Nutzerdaten als Verpflichtung für die ausstellende Behörde
  - Rechtsprechung des EGMR und EuGH: Transparenz ist essentiell zur Ausübung der Betroffenenrechte
- **Benachrichtigung der Justizbehörden**: Notifizierung an die jeweilige Justizbehörde hinsichtlich der Herausgabeanordnung
  - Notifizierung sollte von der ausstellenden Behörde vorgenommen werden
  - Größere Rechtssicherheit für ISPs, wenn die jeweiligen Justizbehörden Kenntnis von der Anordnung erlangen

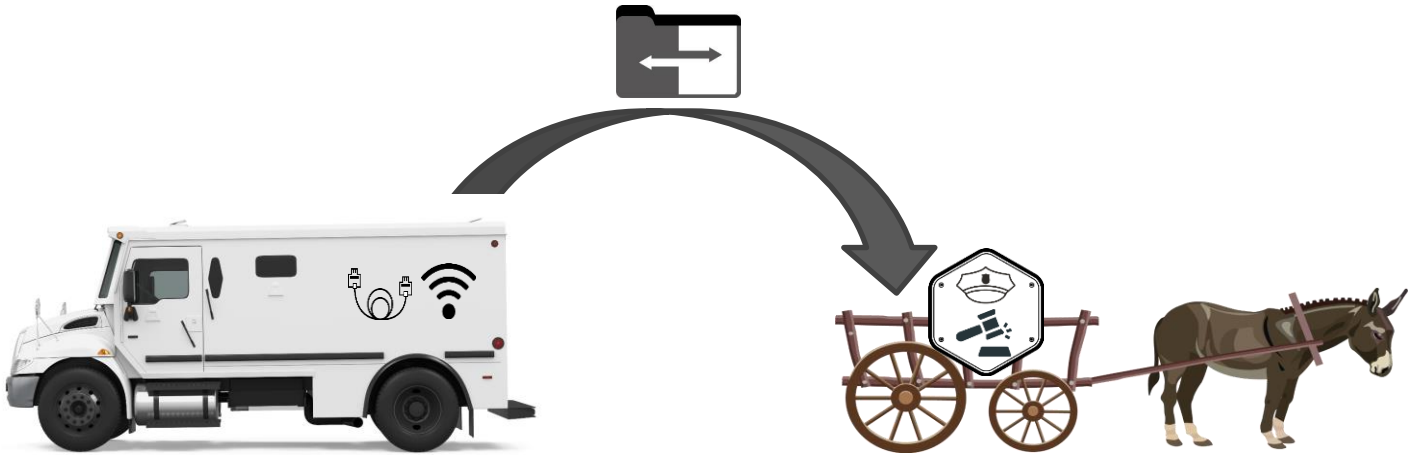
E-Evidence Verordnungsvorschlag
Weitere Anmerkungen und Kritikpunkte

- **Fehlende Ausnahmeregelung für KMU**
  - KMU-Ausnahmen sollten enthalten sein, um die erheblichen administrativen, rechtlichen und finanziellen Belastungen auszugleichen, die durch den Verordnungsvorschlag für die ISPs entstehen werden
- **Fragmentierung der Datenkategorisierung**
  - Kohärenz der Datenkategorien zw. den verschiedenen Rechtsvorschriften (insb. E-Privacy-VO)
- **Datenübermittlung an Drittstaaten**
  - Übereinstimmung mit internationalen Standards (z.B. Budapest Convention bzw. „Umbrella Agreement")
  - Kein ausschließlicher „GAFA"-Fokus
- **Die Reaktionszeiten sind nicht realisierbar**
  - Die Durchführung einer Herausgabeanordnung sollte „unverzüglich" und nicht innerhalb einer vorgegebenen Frist erfolgen

E-Evidence Verordnungsvorschlag
Weitere Anmerkungen und Kritikpunkte

- **Sanktionen nach Vorbild der DSGVO sind unverhältnismäßig**
  - Drakonische Sanktionen verleiten zu einer überschießenden und unüberlegten Datenbeauskunftung – Spannungsverhältnis DSGVO
- **Transparenz**
  - Veröffentlichung von Statistiken über die erteilten Anordnungen
  - ISPs sollten freiwillig Transparenzberichte veröffentlichen dürfen
- **Kostenersatz**
- **Schutz verschlüsselter Daten**
  - Es muss klargestellt werden, dass ISPs keine Daten entschlüsseln müssen
  - Die Übertragung verschlüsselter Daten birgt das Risiko einer ausufernden Datenbeauskunftung

Hohes EU-weites Sicherheits- und Transparenzniveau



Agenda

Über ISPA

Provider-interner Ablauf einer Beauskunftung

Herausforderungen im Kontext der Kooperation ISP – LEAs

E-Evidence-Verordnungsvorschlag

Vorschlag gg. die Verbreiterung von terroristischen Online-Inhalten

EU Vorschlag gegen die Verbreitung von terroristischen Online-Inhalten - Allgemein

Verordnungsvorschlag zur Verhinderung der Verbreitung von terroristischen Online-Inhalten

Entfehrnungsanordnungen
durch die zuständigen Behörden

Hinweise durch die zuständigen Behörden oder z.B. durch Europol

Proaktive Maßnahmen
durch die ISPs

EU Vorschlag gegen die Verbreitung von terroristischen Online-Inhalten - Bedenken

- **Privatisierung der Strafverfolgung**
  - Mit proaktiven Maßnahmen müssen Hosting-Provider über die Rechtmäßigkeit von Inhalten entscheiden
  - Dies würde zu einer übermäßigen Entfernung von legitimen Inhalten führen
  - *Chilling Effect* für Grundrechte und Grundfreiheiten
  - Vage Konzept der „Sorgfaltspflicht"

- **Unmöglich kurze Reaktionszeit**
  - Die Zeitrahmen von **einer Stunde** für die Umsetzung der Entfernungsanordnungen würden zu einer übermäßigen Entfernung gesetzlicher Inhalte führen

EU Vorschlag gegen die Verbreitung von terroristischen Online-Inhalten – Weitere Bedenken

- **Weitere Bedenken**
  - Regelungen über **Kostenersatz** für die finanziell belastenden proaktiven Maßnahmen fehlen
  - Verlässliche **Verifikationsmechanismen** für die Entfernungsanordnungen sind zwingend erforderlich (vgl. E-Evidence)
  - Die **proaktive Datenspeicherung**, ohne eine formelle Anordnung, stellt eine Vorratsdatenspeicherung dar
  - Es bedarf eine **Präzisierung** der Kriterien für die Benennung einer handlungsfähigen zuständigen Behörde
  - Herausforderungen bei **grenzüberschreitenden Entfernungsanordnungen**
  - Ausnahme für Hosting-Diensteanbieter, welche **rein technische Infrastrukturdienste** zur Verfügung stellen

EU Vorschlag gegen die Verbreitung von terroristischen Online-Inhalten – Wiederspruch mit CoE

- **Empfehlung des Europarats über die Rolle und Verantwortlichkeit der Internet-Vermittler (2018)**

  "*State authorities should obtain an order by a **judicial authority** or other independent administrative authority* […] *when demanding intermediaries to restrict access to content*"

  "*State authorities should ensure that notice-based procedures are not designed in a manner that incentivises the take-down of legal content, for example due to **inappropriately short timeframes***"

ispa Internet Service Providers Austria

Vielen Dank!

ispa
Internet Service Providers Austria

E-Evidence Verordnungsvorschlag

- **Erfassten Datenarten**
  - Stammdaten
  - Zugangsdaten
  - Transaktionsdaten
  - Inhaltsdaten

  } Neue Unterteilung von Verkehrsdaten

  → Stammdaten und Zugangsdaten fallen unter das selbe Schutzniveau

- **Adressaten der EPOC und EPrOC**
  - Access-Anbieter, Registrare, Dienste der Informationsgesellschaft iSv Art. 1 lit b) EU 2015/1535, welche ihre Dienste in die EU anbieten

Bedingungen für die Ausstellung v. EPOC und EPrOC

- **EPOC für Stamm- und Zugangsdaten**
  - Für alle strafrechtlichen Vergehen mit einer **FS von mindestens vier Monaten**

- **EPOC für Inhalts- und Verkehrsdaten**
  - Für Straftaten, welche in dem ausstellenden Staat mit einer **FS von mindestens drei Jahren** sanktioniert werden oder
  - Für **Qualifikationen** gemäß Art. 5 Abs. 4 lit b) oder
  - Für die **Exekution** von Urteilen und Haftanordnungen für Straftaten gem. Art. 5 Abs. 4 mit FS von mindestens vier Monaten

- **EPrOC**
  - Für **alle strafrechtlichen Vergehen**
  - **Exekution** von Urteilen und Haftanordnungen von mindestens vier Monaten FS

Ausstellende Stelle für EPOC und EPrOC

- **EPOC – European Production Order Certificate**
  - **Stamm- und Zugangsdaten**
    - Richter, Gericht, Untersuchungsrichter, zuständiger Staatsanwalt
    - Zuständige Behörde nach Genehmigung durch einer der o. g.
  - **Inhalts- und Verkehrsdaten**
    - Richter, Gericht oder Untersuchungsrichter
    - Zuständige Behörde nach Genehmigung durch einer der o. g.
- **EPrOC – European Preservation Order Certificate**
  - **Alle Daten**
    - Richter, Gericht, Untersuchungsrichter, zuständiger Staatsanwalt
    - Zuständige Behörde nach Genehmigung durch einer der o.g.
- **In dringlichen Fällen** auch direkt durch Sicherheitsbehörde und ex-post Genehmigung innerhalb 48h

Notifizierungsverfahren

- **EPOC für Verkehrsdaten**
  - Wohnsitz des Betroffenen nicht im ausstellenden Staat und
  - die ersuchten Daten sind gesetzlich geschützt im vollstreckenden Staat (z.B. Ärzte, Anwälte, Journalisten, Diplomaten usw.)
  - ➢ Konsultation mit den zuständigen Behörden im vollstreckenden Staat vor Ausstellung des EPOC

- **EPOC für Inhaltsdaten**
  - Wohnsitz des Betroffenen nicht im ausstellenden Staat
  - ➢ Kopie der EPOC ergeht gleichzeitig an den ISP und an die zuständige Behörde im vollstreckenden Staat. 10 Tage Reaktionszeit für den vollstreckenden Staat.
  - ➢ Keine aufschiebende Wirkung für den ISP!

Exekution der EPOC & EPrOC

- **EPOC**
  - Innerhalb von 10 Tagen
  - In dringenden Fällen – 6 Stunden

- **EPrOC**
  - Speicherdauer 60 Tage
  - Bei Kenntnis von anstehender EPOC, solang bis die EPOC zugestellt wird
  - Unverzügliche Benachrichtigung des ISP, sofern die Speicherung nicht mehr erforderlich ist

- **Kostenersatz**
  - Sofern im ausstellenden Staat gesetzlich vorgesehen

Durchsetzungsverfahren

- Bei **Nichtbefolgung** durch den ISP
  - Mögliche Durchsetzung durch die zuständige Behörde im vollstreckenden Staat
  - Anerkennung der Anordnung durch die Behörde im vollstreckenden Staat
  - Nach Auskunft sind die Daten an den ausstellenden MS innerhalb von 2 Arbeitstagen zu übermitteln, Ausnahme: „*Immunity or privileges*"
  - Bei weiterer Nichtbefolgung durch den ISP -> Sanktion bis zu 2% des jährlichen weltweiten Umsatzes
- Möglichkeit für den ISP die Anordnung innerhalb von 10 Tagen nach Erhalt **begründet anzufechten**, bei **Verstoß gg. das Recht eines Drittlandes**
- **Überprüfung durch das Gericht** im ausstellenden MS bei Aufrechterhaltung der Anordnung
- **Aufschiebende Wirkung** der gerichtlichen Überprüfung für den ISP

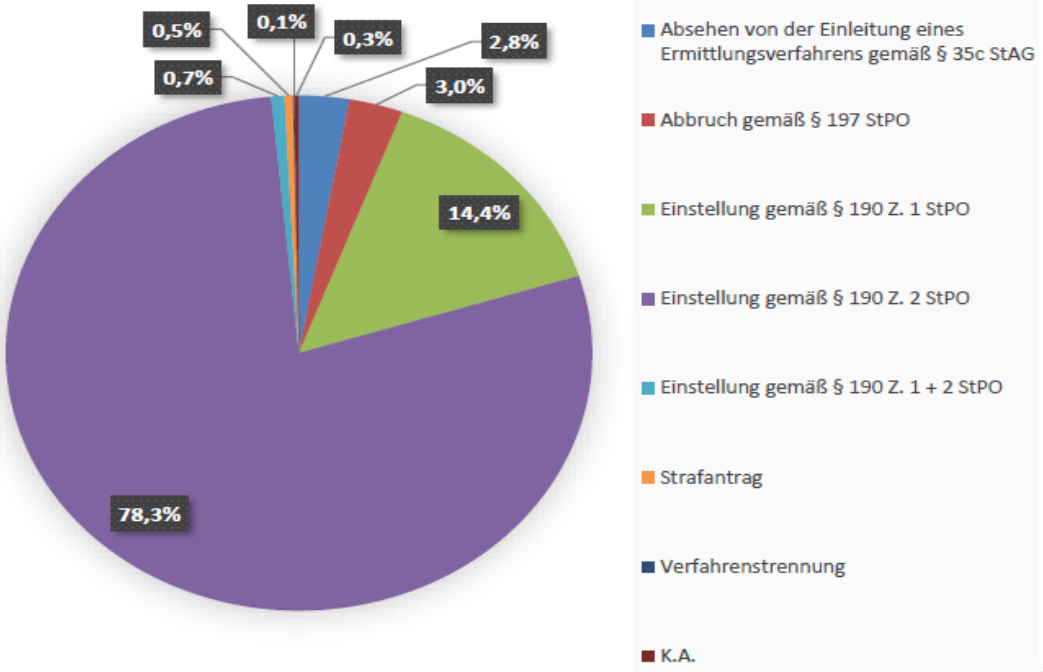
Erfolgschancen einer Beschwerden gg. Executive

Misshandlungsvorwürfe gegen Organe der Sicherheitsbehörden und ähnliche Verdachtsfälle

	2013	2014	2015	2016	**2017**
Bei Staatsanwaltschaften angefallene Fälle[120]	302	299	564	495	509
Einstellung des Ermittlungsverfahrens[121]	570	595	1017	893	932
Abbrechung des Ermittlungsverfahrens (§ 197 StPO)	2	2	15	5	7
Diversion	0	0	0	1	2
Strafantrag/Anklage	5	3	16	18	9
Freispruch	0	1	1	1	3
Schuldspruch	6	2	3	1	8

Quelle: BMVRDJ Sicherheitsbericht 2017

Art der Entscheidung der StA (I)



Quelle: ALES Studie 2018, S. 49

Art der Entscheidung der StA (II)

- Anzahl der **Entscheidungen StA Wien und Salzburg** 2012 -2015
  - **Gesamtzahl** der Entscheidungen StA 1.518
- § 190 **Einstellung des Ermittlungsverfahrens** durch die StA
  - Z. 1: Die Tat ist nicht mit gerichtlicher Strafe bedroht ist oder die weitere Verfolgung des Beschuldigten aus rechtlichen Gründen unzulässig wäre oder
  - Z 2: Es besteht kein tatsächlicher Grund zur weiteren Verfolgung des Beschuldigten
- § 197 StPO **Abbrechung des Ermittlungsverfahrens** gegen Abwesende und gegen unbekannte Täter