Data Retention Austria
Second Attempt

Andreas Krisch <andreas.krisch@vibe.at>

www.edri.org, www.vibe.at

VIBE!AT

- Austrian Association for Internet-Users
- founded in 1999
- Information Society for All
  - Privacy Protection
  - Open Standards
  - Open Access to Information
  - Information Technology accessible for all
  - ...

European Digital Rights – EDRi

- Association of European Privacy and Civil Rights Associations
- founded in 2002
- 29 Member Organisations
- 18 European Countries

- bi-weekly newsletter EDRi-gram since 2003
- German edition since 2006 at www.unwatched.org

Agenda

- Data Retention Austria – First Attempt
- Judgment of the Court of Justice
- Data Retention Austria – Second Attempt
  - The best solution
  - The second-best solution
  - The third-best solution

Data Retention Austria
First Attempt

- 2007: draft law on DR
  - retention period: 6 months
  - serious crime: > 1 year prison sentence
  - access: no court order required
  - access: restricted to “specially authorised persons“

Data Retention Austria
First Attempt

- Arge Daten
  - draft law documents the aim to excessively monitor all aspects of the private lives of citicens
- Constitutional Service Fed. Chancellery
  - beliefs that the draft law in several points is alarming from a constitutional point of view
  - demands to restrict access exclusively to investigation on terrorism and organised crime
- Result:
  - lawmaking process was stopped

Judgement of the Court of Justice

- *"... the provisions of Directive 2006/24 are designed to harmonise national laws on the obligation to retain data (Article 3), the categories of data to be retained (Article 5), the periods of retention of data (Article 6), data protection and data security (Article 7) and the conditions for data storage (Article 8)." (Para. 81)*
- *„By contrast, the measures provided for by Directive 2006/24 do not, in themselves, involve intervention by the police or law-enforcement authorities of the Member States. ..." (Para. 82)*

Judgement of the Court of Justice

- *"Directive 2006/24 thus **regulates operations which are independent of the implementation of any police and judicial cooperation** in criminal matters. It harmonises **neither the issue of access to data** by the competent national law-enforcement authorities **nor that relating to the use and exchange of those data** between those authorities. ..." (Para. 83)*

- → there is no obligation to grant access to or to use the retained data for any purpose!

Data Retention Austria
Second Attempt

- Three Ministries involved:
  - BMVIT: Telecommunications
  - BMJ: Justice
  - BMI: Interior
- BMVIT
  - took the lead
  - asked Ludwig Boltzmann Institute for Human Rights to draft the national DR legislation

Data Retention Austria
Second Attempt

- Ludwig Boltzmann Institute (BIM)
  - has an excellent HR reputation
  - articulated severe fundamental rights concerns with regard to DR
  - insisted to also work on the fundamental rights aspects of DR
  - insisted to draft the entire implementation of the DR directive into national law (including law enforcement aspects, not only telecom-aspects)

DR: the best solution

ceterum censeo

data-retentionem esse delendam!

(Christof Tschohl, BIM)

DR: the second-best solution

- collect
  - the required data, if there is no other possibility than a national implementation of the DR directive
- encrypt
  - the collected data immediately with a government public key
- store
  - the collected data decentralised at ISPs, etc.

DR: the second-best solution

- delete
  - the stored data as soon as possible
- prohibit
  - any access to the stored data
- fight
  - the DR directive, it violates fundamental rights!

DR: the third-best solution

- if there is **no other way** than granting access to LEAs do the following in addition to the second-best solution:
  - restrict access to cases of **really** serious crime
  - establish a **central** decryption department as a single authorised service able to grant access to unencrypted data
  - establish an **effective** control system (Judges, DPA, Parliament, ...)

DR: the third-best solution

- Result:
  - decentralised data storage at ISPs, etc.
  - stored data is encrypted, no access for ISPs
  - LEAs need court-order to access data
  - LEAs send unencrypted request to ISPs
  - ISPs can check legal basis (court order)
  - ISPs encrypt request and search ecrypted data
  - LEAs get encrypted data
  - data is decrypted by central service after checking legal basis

References

- **[EuGH2009]** Judgment of the Court of Justice in Case C-301/06 Ireland v. Parliament and Council, 10.02.2009, http://curia.europa.eu/jurisp/cgi-bin/form.pl?lang=EN&Submit=rechercher&numaff=C-301/06
- **[Tschohl2009]** WZRI – Roundtable Datenschutz & Vorratsdatenspeicherung, 09.03.2009
- **[Krisch2007]** Vorratsdatenspeicherung: Österreich auf dem Weg zur digitalen Überwachungsgesellschaft, 31.05.2007, http://www.unwatched.org/node/495

Thanks for your attention!

Andreas Krisch

andreas.krisch@vibe.at

http://www.edri.org/ http://www.vibe.at/

Donations:

European Digital Rights AISBL

IBAN: BE32 7330 2150 2102

BIC: KREDBEBB