# DATA RETENTION

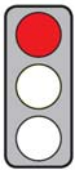
Status: 14 June 2011



## MAIN ISSUES

**Objective of the Report:** The Commission evaluates the Member States' application of the Data Retention Directive, its benefit and impact.

**Parties affected:** Providers and users of telecommunications services.



**Pros:** –

**Cons:** (1) Data retention infringes the fundamental rights to privacy (Art. 7 CFREU) and data protection (Art. 8 CFREU) and the freedom to choose an occupation or to conduct a business (Art. 15 and 16 CFREU).

(2) The Commission does not draw any conclusions from its assessment of the impact data retention has on fundamental rights.

(3) The Commission intends to institute infringement proceedings against Member States which have not yet implemented the – even in the Commission's view – inadequate Directive.

## CONTENT

### Title

**Report COM(2011) 225** of 18 April 2011: Evaluation report on the **Data Retention Directive** (Directive 2006/24/EC)

### Brief Summary

Articles in brackets refer to the Directive 2006/24/EC unless otherwise provided for.

- **Background and objective**
  - The Data Retention Directive (2006/24/EC) stipulates that providers of fixed network telephony, mobile telephony and internet services are obliged to retain traffic and location data of users (Art. 3). The purpose of this is the investigation, detection and prosecution of "serious crime" (Art. 1).
  - In detail, providers are to be obliged to:
    - retain the data for a period of 6 months to 2 years (Art. 6 and Art. 12),
    - provide these to the "competent national authorities" only in specific cases (Art. 4),
    - comply with data security requirements, e.g. taking measures against data loss or destroying data upon the expiry of the data retention period (Art 7 and Art. 9).
  - The objective of the Commission's Report is, in particular, the evaluation of:
    - the Member States' application of the Directive;
    - the value and role of data retention (DR) for criminal justice and prosecution;
    - the impact of DR on providers and users and
    - the impact of DR on fundamental rights.
- **Application of the Directive by Member States**
  - **Missing transposition**
    - Member States were required to transpose the Directive
      - for fixed network telephony and mobile telephony by 15 September 2007 and
      - for internet services by 15 March 2009.
    - Five Member States did not transpose the Directive at all.
      - Austria and Sweden are still in the process of discussing drafts of national legislation.
      - In Germany, Romania and the Czech Republic national constitutional courts annulled the transposing measures.
  - **Purpose of data retention and data access**
    - In transposing the Directive requirements into national legislation, Member States regulated the purpose ("investigation, detection and prosecution of serious crime") and data access differently.
      - In eight Member States the scope of the purpose and data access is defined more broadly than required by the Directive (e.g. to combat not only serious crime).
    - The lack of a consistent EU-wide purpose definition
      - has an impact on the frequency of authorities requesting data and the relating costs accruing to providers and
      - impairs the "foreseeability" of data processing, which is a requirement in light of the fundamental right to privacy.

Authors: Marcus Schwenke and Benedikt Langner | schwenke@cep.eu
CEP | Kaiser-Joseph-Straße 266 | 79098 Freiburg | Germany | Telephone +49 (0)761 38693-105 | www.cep.eu

- The number of authorities having access to data varies in Member States. It ranges from very limited access for police and prosecutors only, to broader access for secret services and military, right up to an inclusion of tax, customs and border authorities.
- Also the requirements regarding the data access procedure are different: ranging from the requirement of the permission of a judge to a written notice requirement only.

– **Retention periods**
- Member States have specified different retention periods; in parts they even differ with respect to the single data categories (e.g. telephony or internet data).
- Different periods led to a "limited" legal certainty and foreseeability of data procession for providers and citizens, providing or using services in more than one Member State.

– **Statistics**
- The Member States provisions regarding statistical data to be processed to the Commission (Art. 14) deviate from each other in terms of scope and detail.
- Several Member States have either "misinterpreted" the sources of the statistical data or not processed any data at all.

► **Value and role of retained data in criminal justice and law enforcement**
– Although the evidence in the form of "statistics and examples provided (…) is limited in some respects", according to the Commission, they nevertheless "attest to the very important role of retained data for criminal investigation" (p. 31).
– According to the Commission, "most Member States" deem DR still necessary:
- Evidence trails can be better used and activities and links between suspects discerned more easily.
- With certain types of crime, notably cyber crime, the retrieval of retained data is the only possibility to initiate criminal investigations.
– In 2008 and 2009, an aggregate 2.6 million retained data requests were submitted in 19 Member States, whereby mainly recent data were requested:
- Over 90% of the requests concerned data which was six months old at the most.
- Over 70% of the requests concerned data which was three months old at the most.
– According to the Commission, most Member States prefer DR to the "quick freeze" procedure which they deem inadequate.
- Under the "quick freeze" procedure, providers only have to retain data relating to suspects when issued with a court order requiring them to do so.
- It does not ensure the retention of "historical data" originating from the time before the court order.
– According to the Commission, "some Member States hold the view that "anonymous prepaid SIM cards" impede or prevent the identification of criminals.

► **Impact of data retention for providers and consumers**
– According to the Commission, the Directive has no quantifiable or substantial effect on consumer prices for electronic communications services and does not change consumer behaviour.
– The Member States' regulations as to the reimbursement of DR costs deviate from each other. The Commission admits that it "has not fully achieved" its aim of establishing a level playing field in Member States (p. 28).
– Due to the high fixed costs of DR, it proved particularly "problematic" for "smaller" providers to comply with their supervising obligations and to ensure the required security measures are in place (p. 9). "Large" providers, however, could allocate the high fixed costs to a larger number of data sets and thus achieve economies of scale. To this end, Finland and the United Kingdom have released small providers from the DR requirement because the related costs "would outweigh the benefits".

► **Implications of data retention for fundamental rights**
– According to the Commission, the relevant jurisdiction requires that "in practice", any limitation of the fundamental right to "respect private and family life" (Art. 7 European Charter of Fundamental Rights, "CFREU") and the fundamental right to the protection of personal data" (Art. 8 CFREU) must:
- be defined precisely and in such a way that the parties addressed by the law can adjust their conduct to it;
- be necessary to achieve an objective of general interest or to protect the rights and freedoms of others;
- be proportionate to the desired aim; and
- preserve the essence of the fundamental rights concerned.

► **Commission's conclusions and prospect**
– Although the Directive failed its objective of harmonising DR, the Commission insists on transposing the current Directive in Member States which are in default. If required, it intends to enforce the Directive through infringement proceedings.
– The Commission wishes to ensure that "any future retention proposal respects the principle of proportionality" (p. 32).

- It wishes to examine the necessity of harmonisation for:
  - the purpose limitation of DR and the types of crime for which retained data may be used,;
  - the group of authorities having access to retained data;
  - the mandatory retention period and
  - the reimbursement of the providers' DR costs.
- Moreover, it considers:
  - reducing retention periods;
  - developing an EU-wide concept for data retention which "might complement" data retention;
  - developing improved evaluation processes for future DR rules as "reliable quantitative and qualitative data are crucial in demonstrating the necessity and value of security measures such as data retention".
- The Commission deems the registration requirement for the use of anonymous prepaid SIM cards unnecessary.

### Statement on Subsidiarity by the Commission

The Commission does not address the issue of subsidiarity directly. However, it states that the EU should ensure that "high standards for the storage, retrieval and use of traffic and location data are consistently maintained" (p. 1).

### Policy Context

The Directive on data protection in the electronic communications sector (2002/58/EC) and the general data protection Directive (95/46/EC) allow Member States in principle to adopt DR legislation. According to the Commission, this led to unfair conditions of competition. In the aftermath of the terrorist attacks in Madrid (2004) and London (2005), in 2006 the DR Directive (2006/24/EC) was adopted.
In Germany it was transposed in 2007 under the new German law „*Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG*". In 2010, the German constitutional court declared the implementation measures in §§ 113a, 113b German Telecommunications Act and § 100g (1) German Code of Criminal Procedure unconstitutional (1 BvR 256/08).

### Options for Influencing the Political Process

Leading Directorate: DG Internal Affairs

## ASSESSMENT

### Economic Impact Assessment

#### Ordoliberal Assessment

The Commission itself admits that the Directive's aim to harmonise DR rules has failed. Therefore, **it is not comprehensible why the Commission wishes to institute infringement proceedings against Member States which have not yet transposed the – even in the Commission's opinion – inadequate Directive**. Far preferable would be if it could be allowed to delay transposition until the Directive has been revised or repealed.

#### Impact on Efficiency and Individual Freedom of Choice

Different regulations regarding data retention increase the compliance costs of providers who are active in several different Member States at the same time. If the use of communications data for law enforcement purposes is necessary at all, it should be harmonized at EU level.
Rules regarding reimbursement which burden small and medium-sized enterprises (SMEs) disproportionately, distort competition. In contrast to large companies they can create economies of scale only to a limited degree.

### Legal Assessment

#### Competence

The Directive was based on the single market legislation (ex-Art. 95 TEC; now Art. 114 TFEU). Although the choice of the legal basis is highly controversial, the Report does not address this issue. According to its wording, the DR serves the purpose of prosecution (Art. 1). A revised Directive, therefore, would have to be based on the rules regarding police and judicial cooperation (different view: ECJ, C-301/06).

#### Subsidiarity

In cases of serious crime, authorities substantially depend on international and cross-border cooperation. Consequently, regulations for the use of telecommunications data to prosecute serious crimes can be better adopted at EU level.

#### Proportionality

The Report is unable to remove concerns regarding DR's suitability for combating serious crime. For instance, the German Federal Commissioner for data protection is right in referring to the fact that the majority of offenders normally have an exceptionally good knowledge of electronic communication and of possibilities to

circumvent data retention and to erase tracks (statement of 31 October 2008, p. 4). In particular, criminal methods such as the use of anonymous prepaid SIM cards call the efficiency of DR into question. As most of the requests made by authorities refer to mobile telephony data and in many Member States there is no obligation to register prepaid SIM cards, it is incomprehensible why the Commission sees no need for action in this acute field.

Moreover, it remains highly questionable whether data retention is necessary at all: the "quick freeze" procedure is an instrument that interferes with the fundamental rights to a much lesser degree but can help achieve the objective just as well. The statements of some unnamed Member Stated quoted in the Report, alleging that the "quick freeze" procedure is not an adequate alternative to DR because this type of data storage does not provide for historical data, is not convincing. In 2007, before the DR had been in introduced to Germany, only 2% of investigators' requests came to nothing due to deleted data (Max-Planck-Institut „*Rechtswirklichkeit der Auskunftserteilung über Telekommunikationsverbindungsdaten nach §§ 100g, 100h*", 2008, p. 254). The Report equally ignores the fact the "quick freeze" proved its value in the USA, which therefore did not introduce an EU-like DR.

The Report clearly shows that a retention period of up to 2 years is not necessary, especially as 90% of the requests concerned data that was less than 6 months old.

**The Commission does not draw any conclusions from its understanding that the interference of DR with fundamental rights** – of both users and providers – **must be proportionate to the stated objectives** and must respect the essence of fundamental rights (p. 29; s. also ECJ, No. 92/09). **The disadvantages resulting from DR totally outweigh its benefits:** on the one hand, there is the registration of highly private life areas of the entire population for no particular reason. Moreover, the registration costs are not allocated to providers in a consistent manner. On the other hand, there is a very limited advantage to be gained from DR serving as a protection of legal interests. This weighs particularly heavy as the Commission fails to present a statistical evidence of the Directive's benefits, despite its considerable relevance for fundamental rights. For instance, it admits to not having reliable quantitative data proving the necessity and value of safety measures such as DR (p. 19). The Commission notably misjudges that an insignificant improvement of the detection rate argues against the value of DR: according to a study of the German federal bureau of criminal investigation, in 2005 only 381 crimes remained unsettled due to missing data (Eva Mahnken, *Mindestspeicherungsfristen für Telekommunikationsverbindungsdaten*, p. 4). In contrast to these 381 cases, there are about 6.4 million crimes, of which about 2.9 million could not be settled. As a result, the detection rate would be improved by only 0.006% through DR.

Furthermore, the Report ignores the fact that obviously there is no detectable link between the use of DR and the crime rate: for instance, in 2008 almost half a million requests were filed in France and Great Britain while only 13,000 in Germany, and yet there was no significant difference in the development of crime in these countries.

### Compatibility with EU Law

**The DR Directive infringes the fundamental rights to privacy (Art. 7 CFREU), data protection (Art. 8 CFREU) and the freedom to an occupation or to conduct a business (Art. 15 and 16 CFREU) because the intervention is not proportionate**, as explained above.

Besides, the Directive infringes – as the Commission itself indirectly admits – the principle that a fundamental right restrictions (*Grundrechtsschranke*) must be defined both precisely and foreseeably (ECJ, C-465/00). For the Directive's definition of the DR requirement not only lacks a clear purpose but also a precise determination of who should be entitled to access the data concerned. The Commission's intended harmonisation could be helpful here.

### Compatibility with German Law

The German constitutional court has ruled that the Directive is not a priory inconsistent with Art. 10 (1) German Basic Law (GG) and could in principle be transposed in line with the Basic Law (1 BvR 256/08). The prerequisite for this is that the data retention period must be no longer than 6 months, the retention without any specific reason remains an exception and the data may be used for good cause only.

## Alternative Action

The DR Directive should be repealed. It should be replaced by the "quick freeze" procedure subject to which national authorities access user data only in compliance with high data protection standards.

## Conclusion

The disadvantages resulting from the Data Retention Directive totally outweigh its benefits. Its provisions infringe the fundamental rights to privacy (Art. 7 CFREU), to data protection (Art. 8 CFREU) and the freedom to choose an occupation or to conduct a business (Art. 15 and 16 CFREU). The Commission does not draw any conclusions from its evaluation of the impact DR has on fundamental rights. It is therefore not comprehensible why the Commission intends to institute infringement proceedings against Member States which have not yet transposed the – even in the Commission's opinion – inadequate Directive.