www.jusletter-it.eu

Jurius

No General Obligation for Data Retention

ECJ – The Members States may not impose a general obligation to retain data on providers of electronic communications services. EU law precludes a general and indiscriminate retention of traffic data and location data, but it is open to Members States to make provision, as a preventive measure, for targeted retention of that data solely for the purpose of fighting serious crime, provided that such retention is limited to what is strictly necessary. (Judgements C-203/15 and C-698/15)

Category: News
Region: EU
Field of law: Data Protection

Citation: Jurius, No General Obligation for Data Retention, in: Jusletter IT 18 May 2017

ISSN 1664-848X, http://jusletter-it.weblaw.ch, Weblaw AG, info@weblaw.ch, T +41 31 380 57 77 EDITIONS WEBLAW

[Rz 1] In the Digital Rights Ireland judgment of 2014 (Joined Cases: C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others, see Press Release No 54/14), the Court of Justice declared invalid the Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (OJ 2006 L 105, p. 54) on the ground that the interference, by the general obligation to retain traffic data and location data imposed by that directive, in the fundamental rights to respect for privacy and the protection of personal data was not limited to what was strictly necessary.

[Rz 2] Following that judgment, two references were made to the Court in relation to the general obligation imposed, in Sweden and in the UK, on providers of electronic communications services to retain the data, relating to those communications, retention of which was required by the invalidated directive.

[Rz 3] On the day following delivery of the Digital Rights Ireland judgment, the telecommunications company Tele2 Sverige informed the Swedish Post and Telecom Authority that it had decided that it would no longer retain data and that it intended to erase data previously recorded (Case C-203/15). Swedish law requires the providers of electronic communications services to retain, systematically and continuously, and with no exceptions, all the traffic data and location data of all their subscribers and registered users, with respect to all means of electronic communication.

[Rz 4] In Case C-698/15, Mr Tom Watson, Mr Peter Brice and Mr Geoffrey Lewis brought actions challenging the UK rules on the retention of data which enable the Secretary of State for the Home Department to require public telecommunications operators to retain all the data relating to communications for a maximum period of 12 months, with the provision that retention of the content of those communications is excluded.

[Rz 5] In references for a preliminary ruling made by the Kammarrätten i Stockholm (Administrative Court of Appeal, Stockholm, Sweden) and the Court of Appeal (England and Wales, Civil Division, UK), the Court is requested to state whether national rules that impose on providers a general obligation to retain data and which make provision for access by the competent national authorities to the retained data, where, inter alia, the objective pursued by that access is not restricted solely to fighting serious crime and where access is not subject to prior review by a court or an independent administrative authority, are compatible with EU law (in particular the Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications [OJ 2002 L 201, p. 37], as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 [OJ 2009, L 337, p. 11] read in the light of the Articles 7, 8 and 52(1) of the Charter of Fundamental Rights of the European Union).

[Rz 6] In its judgment, the Court's answer is that EU law precludes national legislation that prescribes general and indiscriminate retention of data.

[Rz 7] The Court confirms first that the national measures at issue fall within the scope of the directive. The protection of the confidentiality of electronic communications and related traffic data guaranteed by the directive, applies to the measures taken by all persons other than users, whether by private persons or bodies, or by State bodies.

[Rz 8] Next, the Court finds that while that directive enables Member States to restrict the scope of the obligation to ensure the confidentiality of communications and related traffic data, it cannot justify the exception to that obligation, and in particular to the prohibition on storage of data laid down by that directive, becoming the rule.

[Rz 9] Further, the Court states that, in accordance with its settled case-law, the protection of the fundamental right to respect for private life requires that derogations from the protection of personal data should apply only in so far as is strictly necessary. The Court applies that case-law to the rules governing the retention of data and those governing access to the retained data.

[Rz 10] The Court states that, with respect to retention, the retained data, taken as a whole, is liable to allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained.

[Rz 11] The interference by national legislation that provides for the retention of traffic data and location data with that right must therefore be considered to be particularly serious. The fact that the data is retained without the users of electronic communications services being informed of the fact is likely to cause the persons concerned to feel that their private lives are the subject of constant surveillance. Consequently, only the objective of fighting serious crime is capable of justifying such interference.

[Rz 12] The Court states that legislation prescribing a general and indiscriminate retention of data does not require there to be any relationship between the data which must be retained and a threat to public security and is not restricted to, inter alia, providing for retention of data pertaining to a particular time period and/or geographical area and/or a group of persons likely to be involved in a serious crime. Such national legislation therefore exceeds the limits of what is strictly necessary and cannot be considered to be justified within a democratic society, as required by the directive, read in the light of the Charter.

[Rz 13] The Court makes clear however that the directive does not preclude national legislation from imposing a targeted retention of data for the purpose of fighting serious crime, provided that such retention of data is, with respect to the categories of data to be retained, the means of communication affected, the persons concerned and the retention period adopted, limited to what is strictly necessary. The Court states that any national legislation to that effect must be clear and precise and must provide for sufficient guarantees of the protection of data against risks of misuse. The legislation must indicate in what circumstances and under which conditions a data retention measure may, as a preventive measure, be adopted, thereby ensuring that the scope of that measure is, in practice, actually limited to what is strictly necessary. In particular, such legislation must be based on objective evidence which makes it possible to identify the persons whose data is likely to reveal a link with serious criminal offences, to contribute to fighting serious crime or to preventing a serious risk to public security.

[Rz 14] As regards the access of the competent national authorities to the retained data, the Court confirms that the national legislation concerned cannot be limited to requiring that access should be for one of the objectives referred to in the directive, even if that objective is to fight serious crime, but must also lay down the substantive and procedural conditions governing the access of the competent national authorities to the retained data. That legislation must be based on objective criteria in order to define the circumstances and conditions under which the competent national authorities are to be granted access to the data. Access can, as a general rule, be granted, in relation to the objective of fighting crime, only to the data of individuals suspected of planning, committing or having committed a serious crime or of being implicated in one way or another in

such a crime. However, in particular situations, where for example vital national security, defence or public security interests are threatened by terrorist activities, access to the data of other persons might also be granted where there is objective evidence from which it can be inferred that that data might, in a specific case, make an effective contribution to combating such activities.

[Rz 15] Further, the Court considers that it is essential that access to retained data should, except in cases of urgency, be subject to prior review carried out by either a court or an independent body. In addition, the competent national authorities to whom access to retained data has been granted must notify the persons concerned of that fact.

[Rz 16] Given the quantity of retained data, the sensitivity of that data and the risk of unlawful access to it, the national legislation must make provision for that data to be retained within the EU and for the irreversible destruction of the data at the end of the retention period.

Judgments of the ECJ C-203/15 of 21 December 2016 in case Tele2 Sverige AB vs. Post-och telestyrelsen and C-698/15 of 21 December 2016 in case Secretary of State for the Home Department vs. Tom Watson and Others

Source: Press Release of the CJ Nr. 145/16 of 21 December 2016