In a landmark decision the European Court of Justice declares the Telecom Data Retention Directive invalid

The Court of Justice of the European Union (ECJ) issued a landmark decision on 8 April 2014 invalidating the retention of telecommunication traffic and location data by telecom service providers and the access to that data by national authorities under the EU Data Retention Directive 2006/24/EC (Directive). The ECJ concluded that the Directive disproportionally interferes with the fundamental rights of European citizens to private life and protection of personal data. The ruling applies retroactively to the moment the Directive entered into force on 3 May 2006. The ECJ has thus removed the legal foundation for the current retention by the telecom service providers of individual's traffic and location data, and the right by the competent authorities to request that data.

Background

The Directive was adopted on 15 March 2006 and relates to the mandatory retention of telecommunication traffic and location data by telecom services providers. According to the Directive, telecom service providers are obliged to store a person's telecommunications data for a minimum of 6 and a maximum of 24 months. Competent authorities (such as the police or security agencies) are subsequently able to request access to details necessary to trace and identify the source of a communication, destination of a communication, the date, time and duration of a communication, the communication device or the location of mobile equipment etc. These data are required to be available to competent national authorities for the purpose of the investigation, detection and prosecution of a serious crime, as defined by each Member State in its national law.
The Directive covers fixed telephony, mobile telephony, Internet access, Internet email and Internet telephony. To date, all 28 EU Member States have notified the Commission about the transposition of the Directive into their national law, with the exception of Belgium and Germany.

The case in question arose in 2006, after the Irish human rights advocacy organisation Digital Rights Ireland sued the Irish State, questioning the legality and constitutionality of Irish data retention legislation. In 2012 the High Court of Ireland referred the case to the ECJ, asking for its opinion. Similarly, in December 2012, the Austrian Verfassungsgerichtshof referred several constitutional cases to the ECJ, initiated by the Kärntner Landesregierung (Government of the Province of Carinthia) and 128 other applicants seeking the annulment of the national provision transposing the Directive into Austrian law. Both cases were joined by the ECJ in one proceeding.

ECJ's reasoning

The ECJ observed that the traffic and location data to be retained make it possible, in particular, to provide very precise information on the private lives of the persons whose data are retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, activities carried out, social relationships and the social environments frequented. By requiring the retention of those data and by allowing the competent national authorities to access those data, the Directive interferes in a particularly serious manner with the fundamental rights to respect for private life and to the protection of personal data.

Data retention may be appropriate for the objectives but is currently disproportionate

The ECJ stated that “although the retention of data required by the Directive may be considered to be appropriate for attaining the objective pursued by it, the wide-ranging and particularly serious interference of the Directive with the fundamental rights at issue is not sufficiently circumscribed to ensure that that interference is actually limited to what is strictly necessary.”

The ECJ found the Directive to be disproportionate since it:

- applies to all individuals, electronic communication and traffic data without differentiation, limitation or exception
- does not provide for objective substantive criteria and procedural conditions for when access by the competent national authorities would be justified
- does not provide for objective criteria to determine the appropriate retention period in order to ensure that it is limited to what is strictly necessary – the minimum and maximum period in the Directive does not distinguish between the categories of data, persons concerned or the usefulness of the data in relation to the objective pursued
- does not provide for sufficient safeguards to ensure effective protection of the data against the risk of abuse and does not ensure the irreversible destruction of the data at the end of their retention period
- does not require the data to be retained within the European Union, with the result that the control over compliance with the requirements of protection and security of data cannot be fully ensured by an independent authority.
Consequences

In a FAQ issued yesterday, the European Commission indicated that after the judgment by the ECJ “national legislation needs to be amended only with regard to aspects that become contrary to EU law” and further indicated that the finding of invalidity of the Directive does not cancel the ability for Member States under the e-Privacy Directive (2002/58/EC) to oblige retention of data.

The Commission bypasses the fact that the ruling applies retroactively to the moment the Directive entered into force. This entails that the national laws implementing the Directive are equally disproportionate. This means that the competent authorities can no longer rely on these implementation laws vis-à-vis the telecom service providers until such time a new or amended law has been adopted. The fact that Member States have the ability under the e-Privacy Directive to oblige retention of data does not alter this conclusion, unless the relevant implementation were to meet all proportionality requirements listed by the ECJ (which seems highly unlikely).

The competent authorities in the EU can fall back on the Cybercrime Convention of the Council of Europe, which enables among others traffic data preservation. However, data preservation is applied only from the moment a suspicion arises and a preservation order is issued with respect to a particular person, whereas data retention guarantees the availability of historical data linked to the case under investigation. The Cybercrime Convention, although signed by all EU Member States, has not been ratified yet by all of them.

Review of Directive

The Directive has been under review since the end of April 2011, after the Commission in its evaluation report on the Directive concluded that EU rules in this area need to be improved among others to ensure a consistent high level of respect for privacy and the protection of personal data. Although there is no precise timetable at present, the expectation is that the Commission will now step up the review in order to remove legal uncertainly created by the ECJ decision.

In the meantime, it seems that telecom service providers will have valid grounds to refuse to further comply with national data retention obligations and to comply with requests of competent national authorities for access to data.

Contact

If you have any questions or require further information regarding this Legal alert please contact:

IT & Data Compliance
Lokke Moerel | T +31 20 577 1648 | E lokke.moerel@debrauw.com
Wanne Pemmelaar | T +31 20 577 1488 | E wanne.pemmelaar@debrauw.com

Regulatory and Criminal Enforcement
Richard van Staden ten Brink | T +31 20 577 1922 | E richard.vanstadentenbrink@debrauw.com