On 8 April 2014, the Court of Justice of the European Union ("CJEU") declared Directive 2006/24/EC (the "Data Retention Directive") invalid.

The judgement was issued in response to a preliminary ruling request from the Irish High Court and the Austrian Constitutional Court, who queried the Directive's validity in light of the fundamental rights to privacy, data protection and freedom of expression guaranteed by the Charter of Fundamental Rights of the EU (the "Charter"). After an examination of the terms of the Directive, the Charter and relevant case law, the CJEU found that the Directive, although pursuing a legitimate aim, constituted a wholly disproportionate restriction on these rights and therefore declared it invalid with immediate effect.

The implications of this action will be of immediate concern for electronic communications providers in Ireland and across the European Union. Although the precise repercussions of the ruling are as yet unclear, this briefing note outlines the key features of the judgement, its immediate effect in Ireland, and the likely future consequences of this ruling for Irish telecommunications providers.

THE JUDGEMENT
The Court began its assessment by examining the provisions of the Directive.

The Court noted that the Directive imposes an obligation on Member States to provide for the retention of an extremely wide range of customer data by telecommunications companies. All traffic data transmitted by any registered user or subscriber via any means of electronic communication is covered. Such data must be retained for a period of six months to two years and must be made available to 'competent national authorities' upon request.

The court assessed the validity of these provisions in light of the rights to privacy, protection of personal data and freedom of expression contained, respectively, in Articles 7, 8 and 11 of the Charter. After finding that the measures contained in the Directive did constitute an interference with the rights to privacy and data protection (Articles 7 and 8), the Court examined their validity in light of Article 52(1) of the Charter, which provides that any limitation on the exercise of the rights and freedoms laid down by the Charter must be provided for by law, respect their essence and adhere to the principle of proportionality.

While the CJEU did acknowledge that the Directive's provisions respected the essence of the rights in question, and confirmed that the stated aim of combatting serious crime did constitute an 'objective of general interest', it held that the measures chosen to achieve this fell wholly short of complying with the proportionality requirement.
In arriving at this conclusion, the Court levelled the following criticisms against the Directive:

» In relation to the persons affected by its provisions, the Directive covers all subscribers and registered users “without any differentiation, limitation or exception”. It thus applies even to persons for whom there is no evidence indicating that their conduct might have even an indirect link with serious crime;

» As regards the right of national authorities to access the information retained, it fails to lay down any objective criterion or substantive and procedural conditions by which to determine the limits of this access, or indeed the parameters of the subsequent use of the data so procured;

» It fails to make national authorities’ access to retained data dependent on a prior review carried out by a court or by an independent administrative body;

» It provides for a blanket retention period for all data of at least six months, without any distinction being made between categories of information on the basis of its possible usefulness for the purposes of combating serious crime;

» It 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; and

» The Court was particularly critical of the fact that the Directive 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 on expiry of the retention period.

In light of these failings, the Court found that the interference caused by the Directive with the fundamental rights to privacy and protection of personal data was “wide ranging, and particularly serious”, acknowledging that while the aim of combating serious crime justifies the retention of some communications data, “such an objective of general interest, however fundamental it may be, does not, in itself, justify a retention measure such as that established by Directive 2006/24/EC”.

The Court therefore declared the Directive invalid with immediate effect.

INITIAL REACTION
On the same day that the Judgement was issued, the European Commission published a FAQ clarifying that national legislation would now need to be amended to the extent that it conflicted with European Law. It also announced that a meeting would be held on 11 April 2014 in Brussels involving representatives from EU Member States as well as telecoms providers.

Commentators in jurisdictions across the EU queried the legal position of electronic service providers pending affirmative action by Member States to amend or repeal national implementing legislation. Aside from the likely consequences of the decision for national legislative provisions, some commentators queried whether the decision could have a “significant impact on the EU reform of data protection law” in general and in particular on the debate regarding the proposed General Data Protection Regulation (Data Protection Digest, 11 April 2014).

THE POSITION IN IRELAND
The Directive was implemented in Ireland by the Communications (Retention of Data) Act 2011 (the “CRDA”).

While the precise provisions of the CRDA do not exactly mirror those of the Directive, in terms of overall scope and effect the two instruments are very similar. At its core, the CRDA is affected by the same fundamental defects that the CJEU were so critical of in relation to the Directive. In particular:

» It lacks the ‘prior review’ mechanism referred to in the judgement;

» It fails to lay down any objective criterion or substantive and procedural conditions by which to determine the limits of a ‘competent authority’s’ access to the data; and

» It provides for blanket retention periods of one or two years that apply to all data of a certain type without distinction on the basis of potential usefulness or of the persons concerned.

In fact, in certain respects, it could be argued that the CRDA goes even further than the Directive. For example, while the Directive provides for a retention period of six months to two years, the CRDA provides for a mandatory blanket retention period of one or two years (depending on the type of data). Any data not accessed in that time must be destroyed after one month has elapsed since the expiry of the retention period. This arguably brings the total retention period possible under the CRDA to twenty five months, one month longer than the maximum of two years set down by the Directive.

IMPACT OF THE DECISION
Notwithstanding the above, the legal status of the Irish Act remains unaffected by the judgement of the CJEU. The CRDA remains in force until repealed or amended by the Irish Legislature, or declared invalid by an Irish court. The decision of the CJEU does not affect the legal status of the CRDA beyond providing a number of grounds on which it may be challenged as unconstitutional or invalid.

Accordingly, while it has been reported that an ISP in Sweden has already taken a decision deleted to delete all retained records and has ceased collecting customer information, from an Irish law perspective the position remains that national electronic communications providers remain technically obliged to comply with its terms until the CRDA is repealed, replaced or overturned.

Until such a time, any service provider whose acts, done in compliance with the terms of the CRDA, are challenged, will still be able to rely on the justifications contained in Sections 2A and 2B of the Data Protection Acts 1988 and 2003 (the “DPA”) to the effect that the processing of the personal data is required by
Data Retention Directive Declared Invalid by EU Court of Justice

Notwithstanding this, it is arguable that service providers would be well advised to refrain from taking any immediate steps in respect of existing data held pursuant to their CRDA obligations, or complying with new disclosure requests made under the CRDA until such time as the position in relation to the CRDA is clarified by the State.

Law for the performance of a function conferred on a person by an enactment, and also Section 8(e), which enables the processing and disclosure of personal data where required by or under any enactment, rule of law or order of a court.