Germany

The Federal Constitutional Court ruled that

- Retention of data for strictly limited uses for prosecution and security purposes is not necessarily a violation of the German Basic Law, and the Directive can be implemented without violating it.
- Retention of data on persons who have committed no offence but who do not know their data is being retained can created a sense of surveillance which could impair free exercise of fundamental rights.
- The duty of storage of telecommunications data for 6 months was disproportionate in the absence of adequate restrictions on the purpose of the use of the data and provisions for transparency (i.e. informing the data subjects where their data is retrieved) and legal protection, judicial oversight and sanctions against violations of rights
- To be constitutional transposing legislation needed to provide for a particularly high level of security
- Data should only be requested for there is at least a suspicion of serious criminal offence (transposing law goes beyond this provision in the Directive) or evidence of danger to security, and data retrieval should be prohibited for certain communications in connection with an emotional or social need which rely on confidentiality. The law therefore violates

Romania

- The transposing law is unconstitutional in its entirety

- State interference with these rights does not contravene ECHR or constitution if it respects certain rules, adequate and sufficient safeguards to protect against potential arbitrary state action. Acknowledgement that state needs 'adequate and efficient legal tools' to control and combat crime.

- Scope is disproportionately broad.

- Scope of data to be retained must be clear, foreseeable and unambiguous to prevent any arbitrariness or abuse – i.e. the data subject must be able to foresee what consequences of a given action may entail. The law includes 'related data necessary for the identification of subscriber or registered user' – this along with the other types of data in scope 'is likely to prejudice, to inhibit the free usage of the right to communication or to expression' by creating a legitimate suspicion of infringement of right to privacy

- No definition of 'threats to national security' for which authorities may get access, nor exhaustive statement of who can access

- Any continuous legal obligation to retain personal data in effect makes the right to privacy disappear, not the justified use of that data

- It threatens to overturn the presumption of innocence and turns all users of electronic communications into suspected terrorists or serious criminals

- The intrusion into the data subject's privacy automatically implies the intrusion into that of the recipient of the call which he made. The recipient has no control over the data subjects actions

Comment: More than the Karlsruhe judgement, this court appears to dispute the essential principle of a permanent obligation to retain personal data for 6 months. It does not say that data retention can never be constitutional. But it is not convinced that DR is an 'adequate and efficient tool' for law enforcement, and it certainly considers the Romanian law as too flexible and opening up possibilities for abuse.