Data retention in the EU following the CJEU ruling – updated April 2015

Country	How the Directive was implemented in the relevant country	The response to the CJEU ruling in the relevant country
Austria	In 2009 the European Commission began proceedings against Austria for breaching EU law by failing to implement the EU Data Retention Directive. These proceedings resulted in the European Court of Justice ruling against Austria in 2010. Austria's reluctance primarily stemmed from major data protection and privacy concerns. In February 2011, Viviane Reding demanded that Austria finally implemented the directive or otherwise faced stiff charges. Therefore, after years of discussions, the Austrian government finally decided to implement the directive. From November 2009 until January 2010 a legislative proposal for an amendment to the *Telekommunikationsgesetz* (TKG) was open for public surveying. The law proposal came from the Ludwig Boltzmann Institute, which was tasked by the ministry for traffic, innovation and technology (BMVIT) to create a law proposal that would try to impact human and civil rights as little as possible. The draft law was subsequently slightly changed by political processes and that amended proposal[i] was enacted by the Austrian parliament on 18 May 2011.There were demonstrations against the Austrian DR implementation on 21April 2011 in two major cities in Austria.[ii]According to that law, from 1April 2012 Austrian providers had to retain their customers' (meta) data for 6 months and had to delete it within another month. Further demonstrations continued on 31 March 2012 in five large cities.[iii] A special mechanism was introduced that allowed law enforcement agencies or public prosecutors to query the retained data that should ensure transparency and exclude misuse, the so-called "Durchlaufstelle" (roughly translated to 'traversing place'). However, the mechanism allowed bypassing of the traversing place, including any logging of the access, if the agent querying the database stated it was very urgent (e.g. in cases of kidnapping). All in all the Austrian data retention law tried to minimise human and civil rights violations but in some areas the implementation could have been better and more restrictive. For example LEA was able to query the database in cases of severe crimes (on the basis of a warrant) but as the Directive did not spell out what constituted severe crimes, Austria defined severe crimes as being all crimes that had a minimum sentence of 12 month in prison. This led to the fact that not only cases of terrorism, organised crime or murder justified the query of the data retention data but also crimes like polygamy. Another problem of the implementation of the directive was that it allowed	On the 8 April 2014, the CJEU declared the Data Retention Directive to be invalid.[xvi] On 12 June a public hearing at the supreme constitutional court was held. There the Austrian government argued that data retention was a valuable tool and negated the view of the CJEU that suspicion-less mass surveillance would violate the ECHR.[xvii] On 27 June 2014 the Austrian supreme constitutional court declared the DRD implementation in Austria to be not proportionate and unconstitutional and void.[xviii] The Austrian court found the implementation to be invalid because it: • violated the fundamental right to data protection; • violated article 8 ECHR; • the Austrian telecommunications law, the Code of Criminal Procedure and the *Sicherheitspolizeigesetz* ("security police law") did not contain sufficient safeguards for the retention, access and security of the retained data. In particular: o numerous precise safeguards in the law were missing, e.g. concerning the exact arrangement of the retention duties, the necessary preconditions for access to the DR data or the duty to delete the DR data; and o data retention's "mean variation" exceeded any previous judgements in scope, concerning the fundamental right to data protection, both in relation to the affected persons (nearly every citizen is affected) as well as the nature of the DR data and the modality of their usage. The court said that measures such as data retention could constitute valid means to prosecute severe crimes, but only then when in conformity with data protection and human rights laws was ensured. The combined Austrian laws challenged here however constituted a disproportionate interference and thereby a violation of the fundamental right to data protection. On the 30 June, the supreme constitutional court's decision was announced by the Federal Chancellor[xix] and the decision came into effect on 1 July.[xx] On the same day, 1 July, the first major provider (T-Mobile) announced that it had already deleted the DR data.[xxi] Other providers claimed this to be a technical challenge and that it would take some time to delete all DR data. On 7 July, most small providers had deleted the data, the big provider "3" announced that it had already started to delete the data. Only the third large provider in Austria had not started to delete the data at the time of writing. On 10 July, the Austrian minister of the interior announced, that "working without data retention data would not make working any easier" and announced, that she planned to create a new law concerning the protection of the state. However, she said, the new law

intermediaries to store the customer data in countries other than Austria.[iv]
Another severe shortcoming of the implementation was the security of the retained data: here the Ludwig Bolzmann Institute for human rights ran out of time in the legislative drafting process. Therefore another law was referenced that was never suited for this particular job. This led to the security of the retained data not being audited by a single ISP during the whole time the Directive was in force in Austria, because the office tasked with auditing the retained data never had enough resources (time, money and skilled technicians) nor did an actual need for them to audit this data arise from the law that was referenced for that very purpose.[v]

The final implementation of the DR directive did not stop the protests. In October 2011 activists in Austria had started an online petition against data retention and to demand a review of all anti-terrorist legislation.[vi] The petition was signed by 106,067 people by 30 May 2012, making it the most successful online petition ever in Austria. The petition was initially launched on 17 October 2011 (offline). [vii] On 14 December 2011, 4471 signatures were handed over to the parliament then the online petition was launched.

On12 March 2012, the Austrian parliament dealt with the petition for the first time[viii]. The parliament passed the petition to the justice committee,[ix] which on 28th of November 2012 decided to do mostly nothing about it: the Directive had already been challenged before the CJEU and the petition's demand for an evaluation of all anti-terror related laws was simply ignored by the committee.[x]

Then, on 15 June 2012, a lawsuit was filed (by three different parties), including one where 11,130 citizens acted as plaintiffs, after the petition was filed but before the parliament dealt with it. It was a constitutional complaint before Austria's supreme constitutional court, challenging the constitutionality of data retention.[xi] Following this complaint, the Austrian supreme constitutional court referred questions to the CJEU for a preliminary ruling.[xii] The supreme constitutional court shared the concerns expressed in the lawsuit and therefore presented the Court of Justice with some questions on 28 November 2012.[xiii]

In June 2012 the Austrian parliament had dealt with the petition against the DR directive, arguing among other things, that it would be wise to wait for the end of the lawsuit first. Whereby the demand for a re-evaluation of all anti-terror related laws was completely ignored and silently dropped.[xiv]

Finally the CJEU declared the DR directive void and passed the case back to the Austrian supreme constitutional court, which on 27 July 2014 declared the DR would not be related to the overturned data retention law.[xxii] On the 30 July, the written court decision was published.[xxiii]

In late September 2014, Austrian Justice Minister Wolfgang Brandstetter (ÖVP) expressed his intention to aim for a data retention comeback, where data access should only be permitted for "very severe crimes". He expressed hope for a joint drafting process for this together with other justice experts from other parties. Minister of Interior Johanna Mikl-Leitner (ÖVP) welcomed the suggestion. The need for DR legislation was now argued with the Islamic State (IS) and possible activities of IS in Austria. The Greens, AK Vorrat and the Austrian Internet Service Providers Association (ISPA) criticised this heavily.[xxiv]

On 26 September 2014, Maria Wittmann-Tiwald, chairwoman of the association of judges' specialized group for fundamental rights, warned of such a hastily drafted amendment. Without evaluation of the exact need for DR data and technical possibilities, the strict fundamental rights conditions set by the CJEU could not be met, she declared. However, she also said that DR could be justified by the fight against "most severe crimes" whereas terrorism would not provide any justification for DR in Austria.[xxv]

On 27 October 2014, Minister of Interior Johanna Mikl-Leitner (ÖVP) announced within the home affairs committee, that a follow up DR regulation was definitely due to be issued. This was again argued on the basis of IS fighters, despite other evidence that DR data had proven to be meaningless in the fight against terrorism in Austria during the time DR data was present.[xxvi]

On 11 November 2014, Minister of Infrastructure Alois Stöger (SPÖ) announced, that he was not planning to reintroduce DR at present but that he would not resist talks about a reintroduction of DR if the Justice and Home Affairs ministries saw a need for it.[xxvii]

In late November 2014, the political party NEOS discovered that nobody felt responsible for controlling whether the old DR data had ever actually been deleted.[xxviii] On 12 December, this then resulted in a motion for a resolution to the National Council for a law that should enable the verification of the deletion of the DR data.[xxix]

	implementation to be in breach of the constitution.[xv]	
Bulgaria	Directive 2006/24/EC was introduced into Bulgarian law via Ordinance # 40 on the categories of data and the procedure under which they would be retained and disclosed by companies providing publicly available electronic communication networks and/or services for the needs of national security and crime investigation. The Ordinance was issued by the State Agency on Information Technologies and Communication (SAITC) and the Ministry of Interior (MoI). On January 29, 2008, Ordinance # 40 was promulgated in the Bulgarian State Gazette. Ordinance # 40 purported to put Bulgarian legislation in conformity with the Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications and amending Directive 2002/58/EC. An appeal to the Bulgarian Supreme Administrative Court (SAC) against Ordinance # 40 was immediately submitted. The adoption of the Ordinance # 40 was said to violate the right to the protection of private life and correspondence. As set by Art. 32, para. 2 of the Constitution, similar provisions shall be introduced by a law – an act issued by the legislative authority. The Ordinance, however, represents secondary legislation restricting this right. In its decision of December 11, 2008, a five-member panel of the SAC repealed in part the challenged Ordinance. Article 5 provides for a "passive access through a computer terminal" by the Ministry of Interior, as well as access without court permission by security services and other law enforcement bodies, to all retained data by Internet and mobile communication providers. The court ruled that the provision did not set any limitations with regard to the data access by a computer terminal and does not provide for any guarantees for the protection of the right to privacy stipulated by Art. 32, Para. 1 of the Bulgarian Constitution. No mechanism was established for the respect of the constitutionally granted right of protection against unlawful interference in his private or family affairs and against encroachments on his honor, dignity and reputation. The court also found that the text of the Art. 5 of the Ordinance, providing that the investigative bodies, prosecutor's office and the court shall be granted access to retained data "for the needs of the criminal process," the security services – "for the needs of the national security", does not provide limits against violations of constitutionally granted rights of the citizens. Reference to specialized laws – such as the Penal Procedure Code, Special Surveillance Means Act, Personal Data Protection Act, which specify conditions	The formal challenge against the data retention provisions came from Ombudsman Konstantin Penchev in April 2014, only a week after the CJEU ruled to declare the 2006 EU directive that authorised such bulk collection invalid. Even though the objective of the data retention directive was one of public interest (namely the prevention, investigation, detection and prosecution of serious crime), it was a "disproportionate and unjustified interference in the rights of citizens," the Ombudsman said. Bulgaria's highest court annulled the country's data retention law on the grounds that it was unconstitutional. The Constitutional Court, in a meeting on 12 March 2015, delivered a judgment in constitutional case № 8/2014, brought by the Ombudsman of the Republic of Bulgaria.[xxxii] In its decision, the Court declared unconstitutional several articles of the Electronic Communications Act, which were based on the annulled Data Retention Directive. Eight judges agreed that the texts in the law are completely unconstitutional, and three that they are partially unconstitutional. The decision is final: there is no right of appeal. Bulgaria's Constitutional Court declared the provisions mentioned above [Art 250d – 250e, 251 and 251 a] of the Electronic Communications Act introducing Directive 2006/24 /EC into Bulgarian law as unconstitutional.[xxxiii] Rapporteur: Judge Ketty Markova. According to the Ombudsman's request, the contested provisions were adopted by the Law on amendment and supplement of the Electronic Communications Law, prom. SG. 17/2010. They introduce an obligation for legal persons providing public electronic communications networks or services, to store all data generated or processed in the process of their activities relating to trafficking messages to govern the terms and conditions for access to these data and those who have access to them. Some of the arguments of the Constitutional Court in the 30-page decision were as follows: • The Bulgarian legislator *has expanded significantly and even exceeded* the *requirements* of the highly criticized (in theory and practice) Directive 2006/24 / EC (Art. 1, § 1), which, treating access to data traffic, it limited to "the investigation, detection and tracking *serious crime,* as defined by the national law of each Member State. " • There is no settled control *on* the *destruction* of data. • Even a legitimate aim is illegal to be achieved at the cost of such a *substantial and disproportionate interference* with fundamental rights. • In certain cases through the legislative technique used by the challenged provisions

	under which access to personal data shall be granted - was not provided either. Furthermore, according to the court, Art. 5 of the Ordinance contradicts the provision of Art. 8 of the European Convention on Human Rights, according to which everybody has the right to respect for his private and family life, his home and his correspondence and the interference of the state in such matters is unacceptable. The exemptions from that principle are exhaustively listed by Art. 8, Para. 2 of the Convention. The court emphasized that national legal norms shall comply with that established principle and shall introduce comprehensible and well formulated grounds for both access to the personal data of citizens and the procedures for their retention. Article 5 of the Ordinance lacked clarity in terms of protection of the right of private and family life, which contradicts the provision of Art. 8 of the ECHR, the texts of the Directive 2006/24/EC, and Art. 32 and 34 of the Bulgarian Constitution.[xxx] As a result, a number of articles of Ordinance # 40 were declared void, but not the act in its entirety. The Bulgarian legislature amended the Electronic Communications Law according to the court's requests and the amended data retention provisions [Art 250d – 250e, 251 and 251 a] have since been in force until March 2015.[xxxi] 1.4. The main objections against the country's law requiring telecommunications service providers to retain user data for at least a year to aid national security and other criminal investigations: • Scope of implementation – not only for serious crimes • Duration of data retention – 12 months • Lack of the guarantees for citizens	the *constitutional provision for judicial review* has been derogated. • There is no procedure for *the citizens to be notified* of when and on what basis they were the subject of data retention According to the CC such a serious interference should be governed in a manner consistent with *the highest possible standards of security*, which the current legal regulation as a whole does not provide. The law should contain precise, clear and predictable rules establishing certain guarantees for protection and security. This could only be achieved with adequate and effective safeguards: 1) the bodies authorized to requests access to data to being able to exercise this power only in specifically and comprehensively regulated by law; 2) precise procedures for obtaining legal sanction for access to data, their use and destruction; 3) legal guarantees for the safety of data, the scope of their use, transparency and legal protection, including the provision of specialized control against unauthorized access; 4) use the data only for constitutionally legitimate purposes; 5) optimization of the maintenance of the data according to the established European standards, national and European practice; 6) ensuring a balance between restrictions and provided remedies. According to the CC only the full and proper execution of all discussed criteria could be considered adequate.
Czech Republic	There has been new data retention legislation in the Czech republic since November 2012. It was implemented after the Czech constitutional court decision in March 2011, which struck down the previous legislation. The court declared the section of the Electronic Communications Act and its implementing legislation unconstitutional and repealed it. According to the court statement, ambiguous definition of data retention rules results in a situation where such "measures as to request and use retained data are being overused by authorities engaged	The Czech government has prepared no response or changes to the current law following the judgment in *DRI*. In the opinion of the Ministry of interior, the Czech implementation of the directive is in accordance with CJEU ruling. ISPs have no problem with this reaction because their costs for retention of the data are reimbursed. Civil society (IuRe) intends to prepare another constitutional complaint based on CJEU decision about the unconstitutionality of mass surveillance but it is not yet known when this will happen.[xxxvi]

	in criminal proceedings for purposes related to investigation of common, i.e. less serious crimes". According to the Court, it will be necessary to consider each individual case in which data have already been requested in order to be used in criminal proceedings one by one, with respect to the principle of proportionality regarding privacy rights infringement.[xxxiv] The new legislation (§ 97/3+4 of the Electronic communication act and changes to many other acts (especially Penal Procedure Code)) was implemented in the weaker variation of the DRD and it reacted to the constitutional court decision (for example 6 month period for data retention, court control, limitation of the crimes, subsidiarity). However, this did not affect the number of applications for the data (in 2013 about 10,000 per month). Even leaving aside the issue that mass surveillance is arguably an unconstitutional interference with human rights, the new legislation ignores the current situation where the Police Act authorizes the police to use the data outside of criminal proceedings. Under the current Police Act, police officers may require data more or less without any limits, without court supervision and without any clearly defined and controlled processes. The Czech legislation[xxxv] is not available in English.	
Denmark	**About the directive:** • Danish data retention law adopted in 2002 in the wake of 9/11. • Law authorizes the Justice Minister to set the legal requirements for telecommunications providers. • The Administrative order for data retention was adopted in September 2006 and took effect in September 2007. • The four year delay was due to (1) Danish rules postponed so they would fully accord with the EU requirements and (2) technical difficulties with specifying workable data retention rules. **Areas where the Danish directive exceeds EU** • ISP session logging - which requires retention of the following data for every 500th internet packet transmitted by the ISP: source and destination IP address, source and destination port number, transport protocol (e.g. TCP or UDP) and timestamp. The session logging must be done at the boundary of the network, where the ISP exchanges internet packets with other ISPs. • For mobile phone communication, the Danish rules require the retention of the first and last cell used during the communication. The Directive only requires the first cell.	**Reaction from the Danish Government on the ruling:** • The Minister of Justice presented a legal analysis of the ruling. • The Ministry of Justice then noted that the CJEU ruling on data retention is based on three elements: 1. *The directive covers all electronic communication for all persons (paras. 57-59).* There is no difference between the Danish law and the directive with respect to the points in paragraphs 57-59. 2. *The directive does not contain objective criteria for access to the retained data (paras. 60-62).* The Danish Administration of Justice Act contains rules for access to the data. A prior court order is required, except in urgent cases, and there must be grounds for suspicion against the individual whose retained data is accessed. Also, access is restricted to cases of a "serious crime", where the main rule is a prison term of six years or more. However, a number of criminal offences with shorter maximum prison sentences than six years are also included, in particular criminal offences where multiple offenders are likely to work together and use electronic communication for their criminal activities. 3. *The retention period is not based on objective criteria (paras. 63-64).* The Ministry of Justice argues that the retention period in the Danish law is based on objective criteria. The retention period is one year for all types of

	• If the internet service is provided through a WiFi hotspot, the geographical location of the hotspot must be registered. • The Directive applies to "publicly available electronic communications services or public communications networks", whereas the Danish rules apply to all providers of electronic communication services on a commercial basis, whether public or not. Only public institutions, workplaces (internet access for their employees) and public educational institutions are excluded from the Danish data retention requirements. A coffee shop providing WiFi access to their customers would be covered by the Danish data retention requirements as a provider of telecom services. According to comments in the 2002 law, the purpose of including non-public providers in the data retention requirements was to ensure a fair level of competition between public and non- public providers. **Controversy?** • The 2002 law containing data retention and other anti-terror provisions was adopted with a 10:1 majority in parliament. • The Danish Institute of Human Rights and the NGO Digital Rights (a founding member of EDRi) raised several objections, including that blanket data retention was in breach of ECHR Article 8, as the requirements for proportionality were not satisfied. Until the CJEU ruling on 8 April 2014, the response from the Danish Ministry of Justice to this objection has consistently been that "to the extent that data retention is an interference with the fundamental rights to privacy under Article 8, this interference is justified as it is necessary and proportional".	data, but the Ministry of Justice cites preparatory work for the 2002 data retention law in which the one-year retention period was justified on ground as that terrorist attacks such as 9/11 are often planned for more than six months, so a retention period of one year would be appropriate. • The Ministry of Justice voluntarily removed Session logging in June 2014 by a revised administrative order (based on the 2002 data retention law). The Danish government maintains that this change was not because of the CJEU ruling, but because the Danish police have been entirely unable to use the data from session logging. • The Danish data retention law still exceeds the requirements of the now invalid Directive, but session logging accounted for at least 90 percent of the retained data, so there has been a sizeable reduction. **New legislation from the government about data retention?** • In 2016, the Danish government plans to propose a revision of the data retention rules. • This could lead to a reduction in data retention, yet that is highly unlikely as the Danish government is overall very in favour of data retention. • The Minister of Justice emphasized that she was in favour of session logging, but any new rules for such would be highly controversial. • In January 2015 it was reported that the Danish government is considering reintroducing session logging.[xxxvii] However, it is not going to happen in this parliamentary session (Oct 2014 - June 2015). In the current session, the Danish government is required to present a proposal for a revision of the Danish data retention law. The draft law for this, just circulated in public consultation, proposes to postpone the revision for another year until 2015-16. The revision has also been postponed in 2010, 2012, and 2013 for 1-2 years at a time. • The reason given for postponing the revision is to wait for a new data retention directive. • The consultation period for the draft law (revision of data retention law) is ongoing. **Legal challenges and reactions from ISPs** • Danish telecom providers and ISPs have not challenged the data retention rules, either formally (in court) or through civil disobedience (as Bahnhof in Sweden). • There have not been any legal challenges to data retention by other groups. • Denmark does not have a constitutional court, so if citizens believe that a law violates the Danish constitution, the Charter of Fundamental Rights or the European Convention on Human Rights, they have to go through the regular court system, a

		procedure which is quite burdensome. • There is not a case challenging the data retention law in Denmark.
Finland	The *Sähköisen viestinnän tietosuojalaki* (Act on the Protection of Privacy in Electronic Communications, law 516/2004) was amended to add sections 14a, 14b and 14c (amendment law 343/2008) that implement data retention. An English translation of the law is available.[xxxviii] The government bill regarding the amendment was HE 158/2007. How it was implemented: • retention time 12 months; • costs to operators are compensated; • but only operators of certain size are obliged to retain data. Data retention was debated publicly and received lot of criticism from NGOs and also from the politicians of the ruling parties. The government bill was reviewed by the Constitutional Law Committee of the parliament (opinion PeVL 3/2008). The Committee did not find any major problems with the constitutionality of the law. In the voting in the parliament, many parliamentarians who voted for the bill defended their position saying this is something that was not necessary but that EU law required it.	Finland has recently finished a reform of communications and Internet related legislation (*tietoyhteiskuntakaari* = Information Society Code; government bill HE 221/2013). The new law entered into force from 1 January 2015. The data retention provisions were transferred into the new code in a modified form (paragraphs 157–159 of the Information Society Code). The following changes were made compared to the previous DR provisions. The effect of the *DRI* ruling can be seen in the separate retention times and the narrowing down of the data types: 1. no reference to the Directive; 2. obligated operators: those with certain size and ordered by the Ministry of Interior to retain the data (previously: no order required) 3. retained data: • services: mobile phone (calls and sms), Internet phone, Internet access (previously also e-mail, landline and some insignificant data services) • what data: user/subscriber name, address, connection ID, identification of the user, type of communication, recipient, date/time, length, device ID, location of the device in the beginning of the communication, address of the access point (unchanged) 4. retention period shortened (previously 12 months): • mobile phone calls and sms: 12 months • Internet access: 9 months • Internet phone: 6 months The draft bill contained the following but it was removed due to criticism from the Constitutional Law Committee of the parliament. It would have allowed retention of metadata produced from “browsing of websites” or “other data” if retention is necessary to identify the user of an email service, Internet phone service or Internet access. “Other data” is not defined. It could mean the content of a message. This and retention of URLs accessed is problematic. The following is new compared to previous law. The Minister of Interior can build a system where the ISPs could store the retained data. Use of the system would be voluntary but it is likely using that system would reduce their costs so it would be likely that the system will be

		used, effectively creating a centralised database for the state. The law does not define any specific safeguards regarding security of or access to this database. The general rule of court permission would probably apply, as well as general data protection rules. At the time of the *DRI* judgment the Constitutional Law Committee was preparing its opinion on the Information Society Code. In the final opinion (PeVL 18/2014), the Committee criticised data retention in general for violating the principle of proportionality, based on *DRI*. However, the Committee also said that data retention can be implemented if its proportionality can be ensured "in other ways" (whatever that means). There is no news about ISPs. They have been probably retaining data all the time. There have been no legal challenges (no Constitutional Court or similar procedure).
Germany	In Germany the implementation exceeded the Directive's requirements in several ways: • Anonymization services had to log IP assignments (not covered by Directive) • Data access not only for prosecuting serious crime but any crime committed via telecommunications (eg IP infringements) • Also for preventing crime and for purposes of intelligence agencies • Identification of subscribers (including users of dynamically assigned IP addresses) and requesting subscriber data permitted "for the prosecution of criminal or administrative offences, for averting danger to public safety or order and for the discharge of the legal functions of the federal and state authorities for the protection of the Constitution, the Federal Intelligence Service and the Federal Armed Forces Counter-Intelligence Office" • Users of prepaid services are (still) required to provide identification data • Subscriber data is (still) to be stored for 1-2 years, otherwise 6 months • IP address of senders and receivers of e-mails were to be stored Implementation was highly controversial and led to mass protests and complaints to constitutional court. Even today polls suggest that more than 70% of the population reject blanket retention (which is not in force).[xxxix] The German Constitutional Court annulled the law in 2010 on the grounds of the German constitution.[xl] The Directive was not re-implemented following the Court decision.	Germany will probably not enact another data retention instrument unless the EU makes it compulsory. The German Minister of the Interior has publicly called on the EU for new data retention legislation.
Ireland	Implemented through the *Communications (Retention of Data) Act 2011*. 24mths retention for telephony; 12mths for internet. Definitions regarding data to be stored are	The Digital Rights Ireland case continues and the 2011 Act remains in force in the meantime.

	taken verbatim from the Directive. Access is internal within police, revenue and army in respect of the following: 1. A member of the *Garda Síochána* not below the rank of chief superintendent may request a service provider to disclose data retained by the service provider where that member is satisfied that the data are required for: (a) the prevention, detection, investigation or prosecution of a serious offence; (b) the safeguarding of the security of the State; and (c) the saving of human life. 2. An officer of the Permanent Defence Force not below the rank of colonel may request a service provider to disclose to that officer data retained by the service provider where that officer is satisfied that the data are required for the purpose of safeguarding the security of the State. 3. An officer of the Revenue Commissioners not below the rank of principal officer may request a service provider to disclose to that officer data retained where that officer is satisfied that the data are required for the prevention, detection, investigation or prosecution of a revenue offence. There is very limited judicial oversight by means of a single paragraph annual report. The powers are extensively used in respect of quite minor crimes and the safeguards of prior internal authorisation are often ignored with retrospective rubber stamping of requests instead.[xli] Data can also be accessed through *Norwich Pharmacal* (third party disclosure) orders, etc., in respect of civil litigation. There was limited debate - it is a minority political issue.	The government is not preparing new legislation. ISPs haven't been asked to delete data or stop collecting by any party as far as people are aware. The 2011 Act as a piece of primary law (rather than delegated legislation) does not automatically fall following the CJEU ruling, though obviously Digital Rights Ireland are arguing that it must now be struck down by the High Court. The Digital Rights Ireland case challenges both the domestic and EU regimes.[xlii]
Netherlands	The directive has been implemented in Dutch law in the *Wet bewaarplicht Telecommunicatiegegevens*.[xliii] The Dutch law is in some aspects more strict, while in other aspects less or equally weak as the Directive. For example, in the Dutch implementation: • There is no direct relationship between the individuals whose data is preserved and the purpose of the preservation. • There is no exception for those that need professional secrecy, e.g. lawyers and doctors. • There are no meaningful boundaries of offences for which the preserved data may be used. Some of the offences have a maximum penalty of six months only,	The response has been as follows: • The bodies that are supposed to enforce the law explained that they will keep on enforcing the law as long as it hasn't been revoked. • The Dutch government announced[xliv] it will prepare an analysis of the current situation (the Dutch law remains applicable, despite the Directive that led to its introduction having been rendered illegal). • The press is reporting that the government will keep enforcing the law.[xlv] • One of the political parties has made a proposal to cancel the Dutch implementation. The proposal attempts to undo the changes to the legal system that were made when data retention was introduced.[xlvi]

	which extends the "serious crime" requirement of the directive. • There is no review by court or some independent body prior to the access to the data. • There has been no justification for the period of retention (which is six months for internet-related data and twelve months for phone-related data). This is problematic as an evaluation of the law by the Dutch government shows that some data is hardly ever accessed. • Not all retained data is deleted after the retention period. • The Dutch government recently proposed to remove the obligation to notify (afterwards) the subscriber whose data has been accessed, removing the subscribers possibility to take the police to court. The Dutch law has seen a considerable amount of opposition when it was proposed, though it was approved by the Senate after "political opportunity overturned scientific rationality" as one of the Senators members justified his change from opposition to support. The Netherlands does not have a constitutional court.	• On 18 November, the Dutch government finally issued its response to the CJEU ruling. The government wishes to retain its current data retention legislation. The Ministry of Security and Justice wrote a letter to the Parliament saying the CJEU's judgments do not affect the Dutch law on data retention directly.[xlvii] • The government intends to remedy the problems that the ruling creates for the Dutch law by making a few cosmetic changes to the national legislation. A request for data now would need to be approved by a judge, while until now the approval of the public prosecutor was sufficient. In addition to that, a request for data older than six months may only be made for "the most serious category of offences with very long prison sentences". The retention periods, twelve months for phone-related data, six months for internet-related data, are to be kept unchanged. • On 1 December, the Dutch EDRi-member Bits of Freedom heated up the public debate by showing the Dutch law may not be executed by the government, nor by providers. The Dutch Constitution stipulates that a law that violates international treaties, such as the EU Charter of fundamental rights, is invalid.[xlviii] The government was quick to respond by saying it would nevertheless enforce this law. A group of organizations, among them internet provider BIT, is taking the government to court, demanding suspension of the enforcement. • There are two initiatives for new legislation in the Netherlands. There's the proposal of GroenLinks ("GreenLeft") that aims to completely revert to the situation prior to 2009 (when there was a data retention of three months). And there is the proposal of the government containing two fixes, but which leaves the fundamental issues untouched. • On 16 February 2015 the Dutch Data Protection Authority (DPA) at the request of the minister of Security and Justice issued advice on the draft bill.[xlix] The Dutch DPA found that the necessity of retaining all telephony and internet data was insufficiently substantiated. The DPA also noted that lack of substantiating the claim of necessity was surprising, as the government has had enough time to do so, given the fact that the law was in force for 4.5 years. The Dutch DPA recommended that the bill should not be presented to Parliament. The DPA noted that the draft bill does not address whether less far-reaching alternatives would achieve the same result. The DPA concluded that the infringement of the private life of virtually all Dutch citizens was disproportionate. It found that three necessary pre-conditions were not fulfilled: the need to inform people that their data has been accessed after a criminal investigation has been finalised; transparency regarding the use of retained data, such as through the release of statistics; and the need for exemptions for those bound by a duty of professional confidentiality. The DPA found that the distinction between the retention of data and the subsequent use of the data does not alter the disproportionality and the general data retention obligation is unlawful.

		• On 11 March 2015 the District court of The Hague annulled the Dutch data retention law with immediate effect.[l] The law still exists, but may not be executed.
		  ○ The court found the safeguards for access to the retained data to be insufficient. The court did not really consider the necessity of the data retention itself, mostly because during the preliminary injunction, the claim that the law was necessary was not rebutted.
		  ○ The Dutch law allows the use of the retained data not just for serious crime. The state's attorneys said that the Public Prosecution will use its power only when proportionate. The judge's response was that it does not matter if you exploit the possibility or not, the fact that the possibility exists is already reason enough to conclude that the current safeguards are unsatisfactory.
		  ○ Additionally, the court determined that insufficient thought has gone into how data is requested. Saving personal information for a lengthy amount of time is a huge infringement on privacy. Therefore, proper safeguards and guarantees are needed when it comes to acquiring access to this data. The judge deems it reasonable that before a request for information is granted, it is reviewed by a juridical entity or an independent administrative entity.
		  ○ Furthermore, the court considered the substantiation of the necessity of the law. The State claims that the data retention law is necessary. This claim was illustrated during the hearing using a number of shocking criminal cases — but they failed to substantiate necessity. The court took this on board as a valid point, but mainly because during the preliminary injunction, this argument was not rebutted.[li]
		• In the days after the courts judgment, all major providers published statements announcing they would no longer retain data based on the annulled data retention law.[lii] The Agentschap Telecom, the authority responsible for enforcing the law, announced it would cease doing so.[liii] The government stated it was still investigating an appeal. The government is expected to send its proposal for a small number of changes to the law to parliament even sooner.[liv]
		• The Dutch government is expected to send a proposal for a review of the law to the parliament soon.

Norway	Norway is not a member of the EU. Norway is nevertheless closely connected to the EU, particularly through the EEA Agreement between the EU and the members of the European Free Trade Association EFTA (Norway, Iceland and Lichtenstein), which means that all EU-legislation which is relevant to the Internal Market (such as the Data Retention Directive was deemed to be), applies. Formally, though, an EU-directive, to become formally binding according to the EEA Agreement, must be accepted by the EEA Committee. This demands that all the EFTA-members must agree. In the case of	The implementation acts were never put into force. Then the CJEU ruling confirmed that the legal arguments against the directive were valid. At first, the Norwegian Prime Minister's reaction was that the CJEU ruling was not necessarily relevant to the Norwegian implementation, because of the safeguards (judicial control etc) in the Norwegian implementation. However, only days later, on 11 April, the Government announced that it would scrap the implementation and rather review whether a

	the Data Retention Directive, Iceland refused to accept it, on grounds of principle and reference to fundamental rights. *De jure*, therefore, the directive is actually not binding on Norway (nor on the other EFTA-states). The Norwegian Government (and Parliament) did, however, take it for granted that the directive would become binding and the implementation legislation was enacted in April 2011. There was quite a massive public debate in advance of the implementation act. There was resistance from almost all the relevant legal and technical institutions/organizations in civil society, countered by an unusually engaged participation and lobbying in the public debate from the various entities in the law and enforcement and intelligence community. Parliament was sharply divided, but the members representing the Labour Party (*Arbeiderpartiet*) and (most of) the Conservative Party (*Høyre*), secured a 89-80 vote in favour of data retention. The retention obligation for the telecommunications operators and the Internet Service Providers, which, with regard to types of data, complied strictly with the directive, was implemented by enacting a revision of the existing Norwegian Electronic Communication Act. The shortest retention period allowed in the directive – six months – was chosen. There was no such retention obligation in existing Norwegian law at the time (apart from so-called "quick freeze"-orders in specific crime investigations – regulated in the general Criminal Procedure Act, as an implementation of Norway's obligations as party to the European Cyber Crime Convention). Therefore, the introduction of the retention obligation also entailed a number of revisions in particularly the Criminal Procedure Act. Some main points were that access to retained data should – as the main rule – only be given to the police subsequent to a court order, and only in cases relating to crime which carries sanctions of at least four years of imprisonment or to other crimes specifically mentioned in the law. The implementation acts have, however, not been put into force, due initially to delays regarding the secondary legislation in which both the technical details pertaining to, *inter alia*, the level of encryption to be applied to retained data, and the question of how the costs of the new retention scheme should be divided. They will not now be put into force due to the ruling from the CJEU.	new, alternate retention scheme was feasible.[lv] No date or plan for this has been announced publicly.
Poland	The Directive was implemented in Poland in 2009. The retention period was equal for	There was no political response to the CJEU ruling. A group of senators prepared a

	both telephone and Internet traffic data and amounted to 24 months from the date of the communication. After this time, a telecom operator or provider was required to destroy transmission data unless otherwise provided by the law. This period was shortened in January 2013 to 12 months. Access to retained data is granted to the Police, national security agencies (Military Police, Military Counter-Intelligence Service, Fiscal Intelligence, Border Guard, Internal Security Agency, and Central Anticorruption Bureau), and judicial authorities. All authorities have the right to access traffic, subscriber and localization data in case of any crime, however trivial (not only in the case of a serious crime as it stands in the Directive). There is no legal threshold for seriousness of a crime or independent oversight of the disclosure of data by telecom providers to the applicants. Costs for the retention, storage, retrieval and security of this data are borne by telecoms operators and providers. The implementation of the Directive was not controversial for the majority of politicians. Despite this fact, in 2011, two complaints concerning the implementation of the Directive to the Polish legal system were lodged in the Constitutional Tribunal. One of them –coming from the Democratic Left Alliance party – was refused (as all MPs' cases are 'redeemed' after an election). The second complaint was submitted by the Ombudsman and the Constitutional Tribunal delivered a judgment 30 July 2014. The judgment was not a direct response to the CJEU ruling, but judges wrote about it in substantiation of the judgment.	proposition of legislation for a new data retention regime. This project was suspended until the verdict of the Constitutional Tribunal. ISPs did not react officially; they still obey the government and store data. On 30 July 2014 the Polish Constitutional Tribunal finally gave its ruling[lvi] on data retention (and other surveillance powers). The tribunal: • did not hold the data retention unconstitutional (in fact the Court couldn't even consider that - it wasn't included in the complaint) • but it said that access to data must be subjected to independent, external control and more safeguards are necessary (eg. closed list of purposes that justify the use of telecommunication data, additional protection for data covered by professional secrecy, strict rules on deleting data that is not necessary); • now the government and parliament have 18 months to change the law - if they fail, all provisions on data retention will become invalid. The ruling does not give precise guidelines on how oversight mechanisms should be shaped (apart from saying that different standards of control should be provided for different types of data and authorities). The Tribunal also avoided dealing with other important "modalities" such as the catalogue of purposes and the list of authorities entitled to use telecommunication data. Note that Articles 49-51 in the Polish Constitution[lvii] provide that the government should not collect an excessive amount of information on its citizens. The court decision did not mention those sections, because they were not in the original complaint.
Romania	The Directive was implemented in Romania by law 298/2008[lviii] with a text closely following the Directive wording. The law 298 was considered unconstitutional by Constitutional Court Decision no. 1258, on 8 October 2009.[lix] After that decision, the government decided to do nothing for 3 years and then in 2012 it adopted, in a short period of time, a new law 82/2012, almost identical to the one declared unconstitutional.[lx] The amended law, 82/2012, was declared unconstitutional by a new decision of the Romanian Constitutional Court on 8 July 2014[lxi].	There has been no public reaction to the CJEU ruling. On the second day after the ruling the Government initiated a new expanding surveillance.[lxii] According to a public statement of the Romanian Secret Service, there exists an internal note of the government, which "analysed the Romanian implementation of the Data retention directive and concluded that it does not breach human rights". However, the data retention law 82/2012 was declared unconstitutional by a new decision of the Romanian Constitutional Court from 8 July 2014[lxiii] following some unconstitutional complaints raised in pending criminal trials. The decision was made on the grounds of both breaching the Romanian Constitution and based on the CJEU decision. The full reasoning has been published in Romanian only.[lxiv]

		The Court unanimously found that the relevant provisions violated the Constitution and had to be abrogated. The decision refers to the CJEU judgment numerous times. The judges stressed that any interference with the right to privacy should be regarded as very serious. It referred to the creation of a feeling of constant surveillance and the potential to create a detailed portrait a person's private life. The Court found the scheme was a disproportionate interference with the rights to privacy, secrecy of correspondence and freedom of expression. It criticized the lack of safeguards and precise rules. It appears that the data retention law is permanently gone. The law enforcement authorities now want a new law on access to the traffic data already retained by the operators based on the e-privacy law.
Slovakia	In accordance with a Slovakian Constitutional Court decision from 23 April 2014, Slovakia has suspended implementing the Data Retention Directive. It did so in proceedings (PL. ÚS 10/2014) initiated by European Information Society Institute (EISi) with support of thirty Members of Parliament. Although the case has been pending before the Court since October 2012, the Court decided to issue this preliminary measure and accept the case for the further review only now.	On 23 April 2014, the Slovak Constitutional Court preliminarily suspended effectiveness of the Slovak implementation of Data Retention Directive. Preliminary suspension of effectiveness means that the retention laws are still formally valid, but have no legal effect until the Court decides on the merits of the complaint. The Court, however, suspended only provisions that are mandating data retention, while leaving other general provisions on access to those information in tact for now. This means that providers of electronic communication will soon be free of any legal obligation to store data about users. Any storage of the meta-data of users will thus need to be limited to general regime of the Directive 2002/58/EC and the Directive 95/46/EC until the Court finally resolves the case. At the same time, however, already collected data will not need to be destroyed, and it stays open to interpretation whether providers *may* or *may not* disclose *these past data* to state authorities upon request.[lxv] A decision is awaited on the merits of the case.
Slovenia	Data retention has been in force in Slovenia since 2007 (telephone data) and 2009 (internet related data) with retention periods of 14 and 8 months respectively (in 2009 retention periods were shortened from previously 24 months). In the new Act on Electronic Communications, adopted to transpose the provisions of the amended telecommunications package, the legislator did not amend the provisions on data retention.[lxvi] The Information Commissioner has concluded that the data retention provisions of the Act on Electronic Communications (ZEKom-1), which came into force on 15 January 2013, do not respect the principle of proportionality and have been transposed into the national law in contrast with the provisions of the Data Retention Directive. The Information Commissioner reasons that huge amounts of data are stored in advance,	The Constitutional Court of the Republic of Slovenia abrogated the data retention provisions of the Act on Electronic Communications (ZEKom-1) in its judgment U-I-65/13-19 of 3 July 2014[lxix], following the constitutional request lodged by the Information Commissioner in March 2013 and CJEU judgment of 8 April 2014 in *Digital Rights Ireland*. The Court abrogated ZEKom-1 articles 162, 163, 164, 165, 166, 167, 168 in 169 and instructed operators of electronic communications to delete retained data immediately after the judgment was published in the Official Gazette. The Court held data retention as disproportionate for the following reasons: • non-selective retention of data constitutes a breach of rights of a large proportion of population that did not provide any reason to justify such this; – blanket data retention does not provide for anonymous use of communications, which is

	regardless of whether a person has fully obeyed the law, without any evidence or analysis that such a measure is necessary and is reflected in a greater impact on the prosecution of criminal offences. The law includes not only serious crimes as in the Directive, but all criminal offences, national security and the constitutional order, the security, political and economic interests of the state and for the purposes of national defence. [lxvii] On 19 March 2013, the Information Commissioner requested the Constitutional Court to annul the data retention provisions of the Electronic Communications Act. The Information Commissioner therefore decided to file a request to the Constitutional Court of the Republic of Slovenia to assess the constitutionality of data retention provisions.[lxviii]	particularly important in cases where untraceable use is necessary (e.g. calling for help in mental distress); • arguments for the selected retention periods (8 months for internet related and 14 months for telephony related data) were not provided nor explained in the legislative preparatory documents; • the use of retained data was not limited to serious crime.
United Kingdom	The Data Retention (EC Directive) Regulations[lxx] partially transposed the Data Retention Directive in 2007. [lxxi] The regulations included only fixed line and mobile telephony. A Government consultation in 2008 proposed the revocation of these regulations and their replacement by the Data Retention (EC Directive) Regulations 2009 (2009 Regulations). [lxxii] At the time Open Rights Group (ORG) and other rights organisations responded to the Home Office consultation expressing concerns regarding human rights compliance. The 2009 Regulations (also secondary legislation) completed the transposition of the Data Retention Directive by extending data retention to cover internet access, internet telephony and email in addition to fixed line and mobile telephony data. The retention of data became mandatory for twelve months. The communications data that had to be retained was set out in a schedule[lxxiii] to the 2009 Regulations. The requirements applied to public communications providers served with a notice by the Secretary of State. Then, three months after the decision in the *Digital Rights Ireland* case, the Government introduced the Data Retention and Investigatory Powers Act (DRIPA), which has replaced the 2009 Regulations (see right column).	Following the CJEU's decision there was debate regarding whether the UK's implementing legislation was void or voidable. ORG and other organisations discussed potential legal action. ISPs continued to retain data on the Government's advice. Over 1,600 people complained to their ISP stating that their data should no longer be retained. On 10 July 2014 the UK Government announced that it was to introduce new emergency data retention legislation. The Government stated that a failure to act meant ISPs would start deleting data. 4,500 people complained to their MP but the Government achieved cross party support for the legislation. The Data Retention and Investigatory Powers Act[lxxiv] (DRIPA) was enacted on 17 July, following three days of Parliamentary debate. Many organisations complained that this denied Parliament the opportunity for proper scrutiny. The retention period was changed to a maximum of 12 months rather than 12 months. Otherwise the content of the legislation is very similar to the 2009 Regulations, including the types of data to be retained.[lxxv] Retention notices are not published so it is unclear whether they now usually require data to be retained for 12 months or a shorter period. Under Part II of the Regulation of Investigatory Powers Act 2000 (RIPA) a wide range of public authorities can obtain access to the retained data, for broad purposes (that are not confined to safeguarding national security or the prevention, detection or prosecution of defined, sufficiently serious crimes). On 22 July 2014 two Members of Parliament, Tom Watson and David Davis (represented by Liberty), announced they were to legally challenge DRIPA by instigating judicial review proceedings.[lxxvi] They argue that DRIPA is incompatible with Article 8 ECHR and Articles 7

		and 8 EU Charter Fundamental Rights. The case is currently underway in the High Court and we expect a decision in summer 2015. Open Rights Group and Privacy International were granted permission to file a joint third party intervention in the case, which they have since filed.[lxxvii] The organisations argue that DRIPA is contrary to EU law, in particular the Data Protection Directive and the E-Privacy Directive. The organisations also emphasise that: • retention notices issued by the Secretary of State are not person- or crime- specific and do not require a connection between the person whose data is being collected and a situation which is liable to give rise to criminal prosecutions; • the notices do not exclude persons whose communications are subject to professional secrecy obligations; and • there is no requirement that data must be retained within the EU. The Counter-Terrorism and Security Act 2015 adds an additional category of data to the data retained under DRIPA, namely data that may identify the IP address of the sender or recipient of a communication.[lxxviii]

This table was prepared by Open Rights Group using information provided by member organisations of EDRi (European Digital Rights). It is not intended to provide a comprehensive survey of every European country or every response to the DRI decision. We would like to express our thanks to all those who contributed.

---

[i] https://www.ris.bka.gv.at/Dokument.wxe?Abfrage=BgblAuth&Dokumentnummer=BGBLA_2011_I_27
[ii] https://www.flickr.com/photos/austrianpsycho/sets/72157629344576126/with/6887340048/
[iii] https://wiki.gegenvds.at/index.php/Pressespiegel
[iv] http://edri.org/edrigramnumber11-14outsourcing-data-retention-us/
[v] https://netzfreiheit.org/wp-content/uploads/2012/11/IfNf_Bericht-VDS_Datensicherheit.pdf (German)
[vi] http://zeichnemit.at
[vii] http://derstandard.at/1318726346107/VIBEAT-Buergerinitiative-fordert-Verbot-der-Vorratsdatenspeicherung
[viii] http://akvorrat.at/BI-Stoppt-die-Vorratsdatenspeicherung-im-Petitionsauschuss
[ix] http://www.parlament.gv.at/PAKT/PR/JAHR_2012/PK0792/index.shtml
[x] http://albertsteinhauser.at/2012/11/28/enttauschendes-ergebnis-zur-burgerinneninitiative-stopp-vorratsdatenspeicherung-im-justizausschuss/ (German)
[xi] http://www.verfassungsklage.at/files/120615_IA_VDS_Konsolidierte_Fassung.pdf Additional documents concerning the constitutional complaint: http://www.verfassungsklage.at/files/Individualantrag_VDS_Verfahrensdokumente_HS_.pdf (German)
[xii] https://www.unwatched.org/20130614_Verfassungsklage_EuGH_verhandelt_ueber_Vorratsdatenspeicherung http://www.verfassungsklage.at/files/120615_IA_VDS_Konsolidierte_Fassung.pdf (German)
[xiii] http://www.vfgh.gv.at/cms/vfgh-site/attachments/5/9/4/CH0007/CMS1363700023224/vorratdatenspeicherung_vorlage_eugh_g47-12.pdf (German)
[xiv] http://edri.org/edrigramnumber10-12data-retention-petition-austria/
[xv] http://www.vfgh.gv.at/cms/vfgh-site/attachments/5/0/0/CH0003/CMS1403853653944/presseinformation_verkuendung_vorratsdaten.pdf (German)
[xvi] http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf
[xvii] http://derstandard.at/2000001965287/Verfassungsgerichtshof-Regierungsvertreter-verteidigen-Vorratsdatenspeicherung (German)
[xviii] http://www.vfgh.gv.at/cms/vfgh-site/attachments/5/0/0/CH0003/CMS1403853653944/presseinformation_verkuendung_vorratsdaten.pdf (German)
[xix] https://www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2014_I_44/BGBLA_2014_I_44.pdf (German)

[xx] https://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Gesamtabfrage&Dokumentnummer=BGBLA_2014_I_44&ResultFunctionToken=7944ba7c-c683-4 (German)
[xxi] http://derstandard.at/2000002549206/T-Mobile-Vorratsdaten-sind-geloescht (German)
[xxii] http://derstandard.at/2000002916788/Innenministerin-Johanna-Mikl-LeitnerArbeit-wird-ohne-Vorratsdaten-nicht-leichter (German)
and http://derstandard.at/2000002913962/Mikl-Leitner-willAufgaben-des-Staatsschutzes-diskutieren (German)
[xxiii] http://www.vfgh.gv.at/cms/vfgh-site/attachments/5/0/0/CH0003/CMS1403853653944/vds_schriftliche_entscheidung.pdf (German)
[xxiv] http://derstandard.at/2000005845186/Vorratsdaten-Abgeschafft-doch-nicht-erledigt (German)
[xxv] http://derstandard.at/2000006107459/Vorratsdatenspeicherung-Expertin-warnt-vor-Novelle (German)
[xxvi] http://derstandard.at/2000006566691/Junge-IS-Anhaengerinnen-als-Vorwand-fuer-Vorratsdatenspeicherung-neu (German)
[xxvii] http://derstandard.at/2000008024055/Vorratsdaten-Stoeger-plant-keinen-neuen-Anlauf-vorerst (German)
[xxviii] http://derstandard.at/2000008670408/Niemand-prueft-Vorratsdaten-Loeschung (German)
[xxix] http://www.parlament.gv.at/PAKT/VHG/XXV/A/A_00843/fnameorig_377774.html (German)
[xxx] http://www.aip-bg.org/documents/data_retention_campaign_eng.htm
[xxxi] See attached Electronic Communications Law, prom. SG. 41/2007, as suppl. SG. 17/2010
[xxxii] http://constcourt.bg/caseannouncements/Post/907 (Bulgarian)
[xxxiii] See Ognyanova, Nelly. Constitutional Court: The provisions of the ECA, introduced Directive 2006/24 - unconstitutional [in Bulgarian] https://nellyo.wordpress.com/2015/03/17/200624-_data_ret_bg/
[xxxiv] https://edri.org/czech-decision-data-retention/
[xxxv] Act 273/2012 Coll (amendment of the data retention acts): http://www.epravo.cz/top/clanky/jake-budou-dopady-zruseni-smernice-o-data-retention-94415.html Public notice (adjustment circuit stored data, transmission of data etc) http://www.epravo.cz/top/zakony/sbirka-zakonu/vyhlaska-ze-dne-17-rijna-2012-o-uchovavani-predavani-a-likvidaci-provoznich-a-lokalizacnich-udaju-19184.html (Czech)
[xxxvi] http://www.epravo.cz/top/clanky/jake-budou-dopady-zruseni-smernice-o-data-retention-94415.html (Czech)
[xxxvii] https://edri.org/danish-government-plans-to-re-introduce-session-logging/
[xxxviii] http://www.finlex.fi/fi/laki/kaannokset/2004/en20040516.pdf
[xxxix] http://www.vorratsdatenspeicherung.de/images/akvorrat_evaluation_backgrounder_2011-04-17.pdf
[xl] http://www.codices.coe.int/NXT/gateway.dll/CODICES/precis/eng/eur/ger/ger-2010-1-005
[xli] http://www.garda.ie/Documents/User/An%20Garda%20S%C3%ADoch%C3%A1na%20ODPC%20Report%20Final.pdf (p64)
[xlii] http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2426208
[xliii] https://zoek.officielebekendmakingen.nl/stb-2009-333.html (Dutch)
[xliv] https://zoek.officielebekendmakingen.nl/h-tk-20132014-72-2.html (Dutch)
[xlv] http://webwereld.nl/overheid/82140-agentschap-telecom-blijft-bewaarplicht-handhaven (Dutch)
[xlvi] https://zoek.officielebekendmakingen.nl/kst-33939-2.html (Dutch) https://zoek.officielebekendmakingen.nl/kst-33939-3.html (Dutch)
[xlvii] http://www.rijksoverheid.nl/documenten-en-publicaties/kamerstukken/2014/11/19/tk-reactie-van-het-kabinet-naar-aanleiding-van-de-ongeldigverklaring-van-de-richtlijn-dataretentie.html (Dutch)
[xlviii] https://www.bof.nl/2014/12/01/kabinet-moet-per-direct-handhaving-bewaarplicht-stopzetten/ (Dutch) https://www.bof.nl/2014/11/20/kabinet-zegt-eigenlijk-bewaarplicht-vrijwel-ongewijzigd-behouden/ (Dutch)
[xlix] https://cbpweb.nl/en/news/dutch-dpa-issues-advice-revision-data-retention-law
[l] the judgment (in Dutch) is available here: http://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBDHA:2015:2498, an unofficial English translation is available here: http://theiii.org/documents/DutchDataRetentionRulinginEnglish.pdf
[li] http://theiii.org/documents/DutchDataRetentionRulinginEnglish.pdf (unofficial translation of the judgment in English)
[lii] http://over.vodafone.nl/nieuwscentrum/nieuws/vodafone-stopt-met-naleving-wet-bewaarplicht, http://tweakers.net/nieuws/101850/vodafone-kpn-telfort-en-xs4all-stoppen-met-uitvoeren-bewaarplicht.html
[liii] http://agentschaptelecom.nl/actueel/nieuws/2015/wet-bewaarplicht-telecommunicatie-buiten-werking-gesteld
[liv] http://www.rijksoverheid.nl/nieuws/2015/03/11/reactie-van-het-ministerie-van-veiligheid-en-justitie-op-het-vonnis-van-de-kortgedingrechter-inzake-de-bewaarplicht.html
[lv] http://www.nrk.no/norge/regjeringen-dropper-dld-1.11663951, https://www.regjeringen.no/nb/tema/transport-og-kommunikasjon/elektronisk-kommunikasjon/datalagringsdirektivet/id666723/ (both in Norweigan)
[lvi] http://trybunal.gov.pl/sprawy-w-trybunale/art/2013-okreslenie-katalogu-zbieranych-informacji-o-jednostce-za-pomoca-srodkow-technicznych-w-dzialani-4/ (Polish) commentary: http://panoptykon.org/wiadomosc/wyrok-tk-musi-byc-niezalezna-kontrola-nad-sluzbami (Polish)
[lvii] http://www.sejm.gov.pl/prawo/konst/angielski/kon1.htm
[lviii] http://www.legi-internet.ro/legislatie-itc/date-cu-caracter-personal/legea-2982008-privind-pastrarea-datelor-de-trafic-informational.html

[lix] http://www.legi-internet.ro/fileadmin/editor_folder/pdf/decision-constitutional-court-romania-data-retention.pdf

[lx] http://apti.ro/proiect-de-lege-retinerea-datelor (Romanian)

[lxi] Press release at: http://www.ccr.ro/noutati/COMUNICAT-DE-PRES-99 (Romanian) the reasoning was not published yet by the Court.

[lxii] http://edri.org/ecj-data-retention-directive-contravenes-european-law/

[lxiii] Press release at http://www.ccr.ro/noutati/COMUNICAT-DE-PRES-99 (Romanian)

[lxiv] http://privacy.apti.ro/decizia-curtii-constitutionale-date-trafic/ (Romanian)

[lxv] https://cyberlaw.stanford.edu/blog/2014/04/first-european-constitutional-court-suspends-data-retention-after-decision-court

[lxvi] https://edri.org/edrigramnumber11-6slovenia-information-commissioner-challenges-data-retention-law/

[lxvii] https://edri.org/edrigramnumber11-6slovenia-information-commissioner-challenges-data-retention-law/

[lxviii] https://edri.org/edrigramnumber11-6slovenia-information-commissioner-challenges-data-retention-law/

[lxix] http://edri.org/slovenia-data-retention-unconstitutional/ 12 and C-594/12

[lxx] SI 2007/2199

[lxxi] House of Commons Standard Note: The Data Retention and Investigatory Powers Bill, SN/HA/6934

[lxxii] SI 2009/859

[lxxiii] http://www.legislation.gov.uk/ukdsi/2009/9780111473894/schedule

[lxxiv] http://www.legislation.gov.uk/ukpga/2014/27/contents

[lxxv] http://www.legislation.gov.uk/ukpga/2014/27/section/2 (the definition of "relevant communications data" refers to data mentioned in the schedule to the 2009 Regulations)

[lxxvi] https://www.liberty-human-rights.org.uk/news/press-releases/liberty-represents-mps-david-davis-and-tom-watson-legal-challenge-government's-

[lxxvii] https://www.openrightsgroup.org/ourwork/reports/submission-filed-by-org-and-privacy-international-in-dripa-case

[lxxviii] http://www.legislation.gov.uk/ukpga/2015/6/section/21