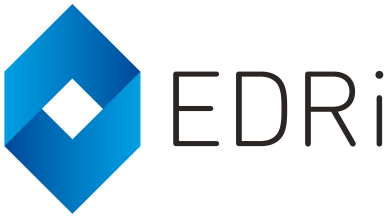
ANNEX. Non-exhaustive list of EU Member States with national legislation contrary to the Digital Rights Ireland Ltd (C-293/12) CJEU ruling.
This list was prepared by European Digital Rights (EDRi), Electronic Frontier Finland (EFFI). IT-Political Association of Denmark (IT-Pol), Open Rights Group (ORG) and Panoptykon.



This Annex contains a list of EU Member States that have laws in force which we consider to be contrary to the **Digital Rights Ireland Ltd** (C-293/12) CJEU ruling. In red we highlighted the parts which are, in our opinion, not in line with the criteria set by the CJEU in the aforementioned case. In green we highlighted the paragraphs which could be in line with the CJEU criteria.

Please note that this list is not exhaustive. We have limited our analysis to the laws of 14 EU Member States: Austria, Bulgaria, Czech Republic, Denmark, Finland, Germany, Ireland, the Netherlands, Poland, Romania, Slovakia, Slovenia, Spain and the United Kingdom. The list highlights national laws which we found to be in flagrant contradiction to the ruling. However, this does not exclude the possibility that the remaining 14 EU Member States, that are excluded from this study, have similar provisions.

ANNEX. Non-exhaustive list of EU Member States with national legislation contrary to the Digital Rights Ireland Ltd (C-293/12) CJEU ruling.
This list was prepared by European Digital Rights (EDRi), Electronic Frontier Finland (EFFI). IT-Political Association of Denmark (IT-Pol), Open Rights Group (ORG) and Panoptykon.

EU Member State	National law	Article of the national law	Relevant paragraph of the CJEU ruling	Text of the CJEU ruling	Explanation of the contradiction with regard to the CJEU ruling
Croatia	Act on Electronic Communications Regulation of the Government of the Republic of Croatia on obligations in the field of national security of the Republic of Croatia for legal and natural persons in telecommunications Act on security and intelligence system in the Republic of Croatia	Articles 109 and 110 Articles 20 - 26	para 58	Directive 2006/24 affects, in a comprehensive manner, all persons using electronic communications services, but without the persons whose data are retained being, even indirectly, in a situation which is liable to give rise to criminal prosecutions. It therefore applies even to persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious crime. Furthermore, it does not provide for any exception, with the result that it applies even to persons whose communications are subject, according to rules of national law, to the obligation of professional secrecy.	The national provisions do not differentiate, limit and/or make exceptions for persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious crime, nor does it provide exceptions for persons whose communications are subject to professional secrecy.
			para 59	Moreover, whilst seeking to contribute to the fight against serious crime, Directive 2006/24 does not require any relationship between the data whose retention is provided for and a threat to public security and, in particular, it is not restricted to a retention in relation (i) to data pertaining to a particular time period and/or a particular geographical zone and/or to a circle of	The national provisions do not require a relationship between the data whose retention is provided for and a threat to public security. There are no restrictions for a particular time period, geographical zone, or persons

				particular persons likely to be involved, in one way or another, in a serious crime, or (ii) to persons who could, for other reasons, contribute, by the retention of their data, to the prevention, detection or prosecution of serious offences.	likely to be involved in serious crime. Data for all persons is retained for 12 months.
			para 61	Furthermore, Directive 2006/24 does not contain substantive and procedural conditions relating to the access of the competent national authorities to the data and to their subsequent use. Article 4 of the directive, which governs the access of those authorities to the data retained, does not expressly provide that that access and the subsequent use of the data in question must be strictly restricted to the purpose of preventing and detecting precisely defined serious offences or of conducting criminal prosecutions relating thereto; it merely provides that each Member State is to define the procedures to be followed and the conditions to be fulfilled in order to gain access to the retained data in accordance with necessity and proportionality requirements.	Competent authorities can obtain access to data, for the purpose of collecting evidence, about duration and frequency of communication, location of communication, location of persons establishing electronic communication and identification of the device for the crimes enlisted in the Act on Penal Procedure and crimes with a prison sentence of more than five years.
			para 62	In particular, Directive 2006/24 does not lay down any objective criterion by which the number of persons authorised to access and subsequently use the data retained is limited to what is strictly necessary in the light of the objective pursued. Above all, the access by the competent national authorities to the data retained is not made dependent on a prior review carried out by a court or by an independent administrative body whose decision seeks to limit access to the data and their use to what is	Provisions of the Act on Penal Procedure (Article 339a) prescribe that the state attorney can access to data only by a court order. Access to data according to the provisions of the Act on security and intelligence system in the

				strictly necessary for the purpose of attaining the objective pursued and which intervenes following a reasoned request of those authorities submitted within the framework of procedures of prevention, detection or criminal prosecutions. Nor does it lay down a specific obligation on Member States designed to establish such limits.	Republic of Croatia is approved by the head of the security-intelligence agency.
			para 64	Furthermore, that period is set at between a minimum of 6 months and a maximum of 24 months, but it is not stated that the determination of the period of retention must be based on objective criteria in order to ensure that it is limited to what is strictly necessary.	The retention period does not distinguish between different kinds of data. The retention period is 12 months for all types of data.
			para 67	Article 7 of Directive 2006/24, read in conjunction with Article 4(1) of Directive 2002/58 and the second sub-paragraph of Article 17(1) of Directive 95/46, does not ensure that a particularly high level of protection and security is applied by those providers by means of technical and organisational measures, but permits those providers in particular to have regard to economic considerations when determining the level of security which they apply, as regards the costs of implementing security measures. In particular, Directive 2006/24 does not ensure the irreversible destruction of the data at the end of the data retention period.	The national law requires the irreversible destruction of the data at the end of the data retention period. However, exception is made for the data about malicious or disturbing phone calls, SMS and MMS messages, and data about secret surveillance of electronic communication networks and services when processed and retained for purposes of competent bodies.
			para 68	In the second place, it should be added that that directive does not require the data in question to be retained within the European Union, with the result that it cannot be held	The national provisions do not expressly require that the data must be retained within the EU.

				that the control, explicitly required by Article 8(3) of the Charter, by an independent authority of compliance with the requirements of protection and security, as referred to in the two previous paragraphs, is fully ensured. Such a control, carried out on the basis of EU law, is an essential component of the protection of individuals with regard to the processing of personal data (see, to that effect, Case C-614/10 Commission v Austria EU:C:2012:631, paragraph 37).	
Denmark	Administration of Justice Act Administrative Order for Data Retention (logningsbekendtgørelsen), 2014	Section 786(4) Chapter 2 (sections 4-9)	para 58	Directive 2006/24 affects, in a comprehensive manner, all persons using electronic communications services, but without the persons whose data are retained being, even indirectly, in a situation which is liable to give rise to criminal prosecutions. It therefore applies even to persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious crime. Furthermore, it does not provide for any exception, with the result that it applies even to persons whose communications are subject, according to rules of national law, to the obligation of professional secrecy.	The Danish data retention requirements, being identical to the annulled directive, do not make any exceptions for persons whose communication are subject to professional secrecy. Moreover, there is no exception for persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious crime.
			para 59	Moreover, whilst seeking to contribute to the fight against serious crime, Directive 2006/24 does not require any relationship between the data whose retention is provided for and a threat to public security and, in particular, it is not restricted to a retention in relation (i)	There is no requirement for a relationship between the retained data and a threat to public security. Specifically, there are no restrictions for a particular time

				to data pertaining to a particular time period and/or a particular geographical zone and/or to a circle of particular persons likely to be involved, in one way or another, in a serious crime, or (ii) to persons who could, for other reasons, contribute, by the retention of their data, to the prevention, detection or prosecution of serious offences.	period, geographical zone, or persons likely to be involved in serious crime. Data for all persons is retained for one year.
			para 61	Furthermore, Directive 2006/24 does not contain substantive and procedural conditions relating to the access of the competent national authorities to the data and to their subsequent use. Article 4 of the directive, which governs the access of those authorities to the data retained, does not expressly provide that that access and the subsequent use of the data in question must be strictly restricted to the purpose of preventing and detecting precisely defined serious offences or of conducting criminal prosecutions relating thereto; it merely provides that each Member State is to define the procedures to be followed and the conditions to be fulfilled in order to gain access to the retained data in accordance with necessity and proportionality requirements.	Competent authorities can obtain access to data about cell ID (location for mobile telephony) and who is using an assigned IP address (internet) for any offence that is subject to public prosecution, irrespective of the type of crime and its seriousness.[i] For the other data types, access is restricted to investigation and prosecution of crimes with a maximum prison sentence of at least six years, as well as a specific list of other crimes with shorter maximum prison sentences. The specific list (shorter sentences than six years) contains crimes, where typically multiple offenders work together, where telecommunication services are likely to be used for

					the crime, and where access to telecommunication data is relevant for the police investigation of the crime.[ii]
			para 62	In particular, Directive 2006/24 does not lay down any objective criterion by which the number of persons authorised to access and subsequently use the data retained is limited to what is strictly necessary in the light of the objective pursued. Above all, the access by the competent national authorities to the data retained is not made dependent on a prior review carried out by a court or by an independent administrative body whose decision seeks to limit access to the data and their use to what is strictly necessary for the purpose of attaining the objective pursued and which intervenes following a reasoned request of those authorities submitted within the framework of procedures of prevention, detection or criminal prosecutions. Nor does it lay down a specific obligation on Member States designed to establish such limits.	Access to the data by competent authorities requires a court order. Normally, this must be obtained prior to access. In urgent situations, it can be obtained after access, but within 24 hours.[iii]
			para 64	Furthermore, that period is set at between a minimum of 6 months and a maximum of 24 months, but it is not stated that the determination of the period of retention must be based on objective criteria in order to ensure that it is limited to what is strictly necessary.	The retention period does not distinguish between different kinds of data. The retention period is one year for all data types.
			para 67	Article 7 of Directive 2006/24, read in conjunction with	There is not specific requirement

				Article 4(1) of Directive 2002/58 and the second sub-paragraph of Article 17(1) of Directive 95/46, does not ensure that a particularly high level of protection and security is applied by those providers by means of technical and organisational measures, but permits those providers in particular to have regard to economic considerations when determining the level of security which they apply, as regards the costs of implementing security measures. In particular, Directive 2006/24 does not ensure the irreversible destruction of the data at the end of the data retention period.	in Danish law for the irreversible destruction of the data after the end of the data retention period. There is only the general requirement in the Danish transposition of Article 6(1) of the e-privacy directive 2002/58/EC that traffic data is deleted or anonymised when no longer needed.
			para 68	In the second place, it should be added that that directive does not require the data in question to be retained within the European Union, with the result that it cannot be held that the control, explicitly required by Article 8(3) of the Charter, by an independent authority of compliance with the requirements of protection and security, as referred to in the two previous paragraphs, is fully ensured. Such a control, carried out on the basis of EU law, is an essential component of the protection of individuals with regard to the processing of personal data (see, to that effect, Case C-614/10 Commission v Austria EU:C:2012:631, paragraph 37).	There is no requirement in Danish law that the data is retained within the European Union.
Finland	Information Society Code (Tietoyhteiskuntakaari), 917/2014, 2015	Section 19, paragraphs 157–159	para 58	Directive 2006/24 affects, in a comprehensive manner, all persons using electronic communications services, but without the persons whose data are retained being, even	There is no requisite of a connection to serious crime. In this respect the law is equal to the

				indirectly, in a situation which is liable to give rise to criminal prosecutions. It therefore applies even to persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious crime. Furthermore, it does not provide for any exception, with the result that it applies even to persons whose communications are subject, according to rules of national law, to the obligation of professional secrecy.	directive. There are also no exceptions regarding professional secrecy.
			para 59	Moreover, whilst seeking to contribute to the fight against serious crime, Directive 2006/24 does not require any relationship between the data whose retention is provided for and a threat to public security and, in particular, it is not restricted to a retention in relation (i) to data pertaining to a particular time period and/or a particular geographical zone and/or to a circle of particular persons likely to be involved, in one way or another, in a serious crime, or (ii) to persons who could, for other reasons, contribute, by the retention of their data, to the prevention, detection or prosecution of serious offences.	There is no requirement for a relationship between the retained data and a threat to public security. Specifically, there are no restrictions for a particular time period, geographical zone, or persons likely to be involved in serious crime. The retention obligation does not apply to all service providers, only the major ones, but they are all nation-wide so there isn't any geographical limitation in this way either.
			para 61	Furthermore, Directive 2006/24 does not contain substantive and procedural conditions relating to the access of the competent national authorities to the data and to their subsequent use. Article 4 of the directive, which governs the access of those authorities to the data retained, does not expressly provide that that access and	According to 157(1) of the law, the data can only be used for detection or prosecution (not prevention) of crimes listed in Section 10 paragraph 6(2) of the Coercive Measures Act. This list

				the subsequent use of the data in question must be strictly restricted to the purpose of preventing and detecting precisely defined serious offences or of conducting criminal prosecutions relating thereto; it merely provides that each Member State is to define the procedures to be followed and the conditions to be fulfilled in order to gain access to the retained data in accordance with necessity and proportionality requirements.	contains a number of clearly serious crimes but with two exceptions. The data can also be used 1) in the case of an unauthorized access to a computer system or 2) in the case of crime with a maximum prison sentence of minimum two years if the act was committed using a “telecommunications address” or “telecommunications device”. According to the Criminal Code, some examples of such offences would include ethnic agitation (hate speech towards minority groups), violation of political freedom (in a political meeting etc.), giving false statement in official proceedings, falsification of evidence, breach of a prohibition to pursue a business, giving of bribes, public incitement to an offence, prevention of worship, lottery offence (organising a lottery without a permit etc.) – when using telecommunications in the act. This is only a partial list, but

					clearly not all of these can be considered serious offences.
			para 62	In particular, Directive 2006/24 does not lay down any objective criterion by which the number of persons authorised to access and subsequently use the data retained is limited to what is strictly necessary in the light of the objective pursued. Above all, the access by the competent national authorities to the data retained is not made dependent on a prior review carried out by a court or by an independent administrative body whose decision seeks to limit access to the data and their use to what is strictly necessary for the purpose of attaining the objective pursued and which intervenes following a reasoned request of those authorities submitted within the framework of procedures of prevention, detection or criminal prosecutions. Nor does it lay down a specific obligation on Member States designed to establish such limits.	Access to the data by competent authorities requires a court order. Normally, this must be obtained prior to access. In urgent situations, it can be obtained after access, but within 24 hours. According to a study from 2009, the permission is almost always granted by the court.[iv]
			para 64	Furthermore, that period is set at between a minimum of 6 months and a maximum of 24 months, but it is not stated that the determination of the period of retention must be based on objective criteria in order to ensure that it is limited to what is strictly necessary.	The Retention period is distinguished according to the type of communication: - mobile phone calls and sms: 12 months - Internet access: 9 months - Internet phone: 6 months. There is no separation according to usefulness or persons.

			para 67	Article 7 of Directive 2006/24, read in conjunction with Article 4(1) of Directive 2002/58 and the second sub-paragraph of Article 17(1) of Directive 95/46, does not ensure that a particularly high level of protection and security is applied by those providers by means of technical and organisational measures, but permits those providers in particular to have regard to economic considerations when determining the level of security which they apply, as regards the costs of implementing security measures. In particular, Directive 2006/24 does not ensure the irreversible destruction of the data at the end of the data retention period.	There is no specific requirement of irreversible destruction of the data after the end of the data retention period. There is only the general requirement in Information Society Code 137(3) that traffic data is deleted or anonymised when no longer needed.
			para 68	In the second place, it should be added that that directive does not require the data in question to be retained within the European Union, with the result that it cannot be held that the control, explicitly required by Article 8(3) of the Charter, by an independent authority of compliance with the requirements of protection and security, as referred to in the two previous paragraphs, is fully ensured. Such a control, carried out on the basis of EU law, is an essential component of the protection of individuals with regard to the processing of personal data (see, to that effect, Case C-614/10 Commission v Austria EU:C:2012:631, paragraph 37).	There is no requirement in Finnish law that the data is retained within the European Union.
Italy	Decreto Legislativo 30 giugno 2003, n. 196 “Codice in	Art. 132, Paragraph	58	Directive 2006/24 affects, in a comprehensive manner, all persons using electronic communications services, but	The law does not differentiate on the basis of the data subject or on

	materia di protezione dei dati personali." (Legislative Decree 30 June 2003, n. 196 "Code concerning the protection of personal data")	1		without the persons whose data are retained being, even indirectly, in a situation which is liable to give rise to criminal prosecutions. It therefore applies even to persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious crime. Furthermore, it does not provide for any exception, with the result that it applies even to persons whose communications are subject, according to rules of national law, to the obligation of professional secrecy.	his/her involvement in serious crimes; neither does it provide exceptions based on professional secrecy.
		Art. 132, Paragraph 1	59	Moreover, whilst seeking to contribute to the fight against serious crime, Directive 2006/24 does not require any relationship between the data whose retention is provided for and a threat to public security and, in particular, it is not restricted to a retention in relation (i) to data pertaining to a particular time period and/or a particular geographical zone and/or to a circle of particular persons likely to be involved, in one way or another, in a serious crime, or (ii) to persons who could, for other reasons, contribute, by the retention of their data, to the prevention, detection or prosecution of serious offences.	There are no such restrictions in the Italian law.
		Art. 132, Paragraph 1, 3 and 4 ter	61	Furthermore, Directive 2006/24 does not contain substantive and procedural conditions relating to the access of the competent national authorities to the data and to their subsequent use. Article 4 of the directive, which governs the access of those authorities to the data retained, does not expressly provide that that access and	There is no restriction to the access and/or use of the data to the prevention, detection or prosecution of precisely defined serious offences. The reference only reads "to inspect and repress

				the subsequent use of the data in question must be strictly restricted to the purpose of preventing and detecting precisely defined serious offences or of conducting criminal prosecutions relating thereto; it merely provides that each Member State is to define the procedures to be followed and the conditions to be fulfilled in order to gain access to the retained data in accordance with necessity and proportionality requirements.	crimes." Article 132 Paragraph 4 provides an exception for paricularly serious crimes such as terrorism, allowing the access by police forces and other subjects for "preventive investigation" and different data retention periods.
		Art. 132, Paragraph 3 and 4 ter	62	In particular, Directive 2006/24 does not lay down any objective criterion by which the number of persons authorised to access and subsequently use the data retained is limited to what is strictly necessary in the light of the objective pursued. Above all, the access by the competent national authorities to the data retained is not made dependent on a prior review carried out by a court or by an independent administrative body whose decision seeks to limit access to the data and their use to what is strictly necessary for the purpose of attaining the objective pursued and which intervenes following a reasoned request of those authorities submitted within the framework of procedures of prevention, detection or criminal prosecutions. Nor does it lay down a specific obligation on Member States designed to establish such limits.	The Italian law does not provide any previous proportionality assessment on the data accessed. As well, no prior review made by a court or an independent authority is required.
		Art. 132, Paragraph	63	Thirdly, so far as concerns the data retention period, Article 6 of Directive 2006/24 requires that those data be	The provisions only differentiate among phone calls, missing calls

		1 and 1-bis		retained for a period of at least six months, without any distinction being made between the categories of data set out in Article 5 of that directive on the basis of their possible usefulness for the purposes of the objective pursued or according to the persons concerned.	and internet traffic metadata, providing different periods of retention,[1] without any reference to the quality of the data.
		Art. 132 Also Art. 31-32.	67	Article 7 of Directive 2006/24, read in conjunction with Article 4(1) of Directive 2002/58 and the second sub-paragraph of Article 17(1) of Directive 95/46, does not ensure that a particularly high level of protection and security is applied by those providers by means of technical and organisational measures, but permits those providers in particular to have regard to economic considerations when determining the level of security which they apply, as regards the costs of implementing security measures. In particular, Directive 2006/24 does not ensure the irreversible destruction of the data at the end of the data retention period.	Art. 31 offers some safeguards regarding the obligation to establish high levels of security for the protection of personal data. However, there is no provision that requires the service provider to destroy the data.
		Art. 132	68	In the second place, it should be added that that directive does not require the data in question to be retained within the European Union, with the result that it cannot be held that the control, explicitly required by Article 8(3) of the Charter, by an independent authority of compliance with the requirements of protection and security, as referred to in the two previous paragraphs, is fully ensured. Such a control, carried out on the basis of EU law, is an essential	There is no provision on this.

1 Article 4-bis Anti-terrorism decree (15/04/2015) derogates to Article 132 Paragraph 1, provisionally extending the retention period for all kind of data to the 31st of December 2016. This provision will cease to apply starting from the 1st of Genuary 2017.

				component of the protection of individuals with regard to the processing of personal data (see, to that effect, Case C-614/10 Commission v Austria EU:C:2012:631, paragraph 37).	
Poland	The Directive was implemented in 2009.		para 41 (+42 and 44)	As regards the question of whether that interference satisfies an objective of general interest, it should be observed that, whilst Directive 2006/24 aims to harmonize Member States' provisions concerning the obligations of those providers with respect to the retention of certain data which are generated or processed by them, the material objective of that directive is, as follows from Article 1(1) thereof, to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law. The material objective of that directive is, therefore, to contribute to the fight against serious crime and thus, ultimately, to public security.	In Poland definition of serious crime was not adopted. The Penal Code provides for the division of different types of crimes, but this framework does not apply to the telecommunication data retention regime. The entitled entities can request telecommunication data in connection with preventing or investigating crimes of all types.
			para 51	As regards the necessity for the retention of data required by Directive 2006/24, it must be held that the fight against serious crime, in particular against organised crime and terrorism, is indeed of the utmost importance in order to ensure public security and its effectiveness may depend to a great extent on the use of modern investigation techniques. However, such an objective of general interest, however fundamental it may be, does	The aim of the national data retention law, besides the objective of fighting against serious crimes, is to search for missing people and implementation of the tasks of certain agencies, such as National Security Agency.

				not, in itself, justify a retention measure such as that established by Directive 2006/24 being considered to be necessary for the purpose of that fight.	
			para 52	So far as concerns the right to respect for private life, the protection of that fundamental right requires, according to the Court's settled case-law, in any event, that derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary (Case C-473/12 IPI EU:C:2013:715, paragraph 39 and the case-law cited).	In Polish law that requirement is not met.
			para 54	Consequently, the EU legislation in question must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards so that the persons whose data have been retained have sufficient guarantees to effectively protect their personal data against the risk of abuse and against any unlawful access and use of that data (see, by analogy, as regards Article 8 of the ECHR, Eur. Court H.R., Liberty and Others v. the United Kingdom, 1 July 2008, no. 58243/00, § 62 and 63; Rotaru v. Romania, § 57 to 59, and S. and Marper v. the United Kingdom, § 99).	The Polish Code of Criminal Procedure provides such safeguards, but they are not applicable to access telecommunication data by police and other agencies.
			para 55	The need for such safeguards is all the greater where, as laid down in Directive 2006/24, personal data are subjected to automatic processing and where there is a significant risk of unlawful access to those data (see, by analogy, as regards Article 8 of the ECHR, S. and Marper	Data protection law provides for general principles such as lawfulness and certain rights of data subjects (e.g. the right to information regarding automatic

				v. the United Kingdom, § 103, and M. K. v. France, 18 April 2013, no. 19522/09, § 35).	processing of data), but there are no safeguards. In particular, there are no legal procedures that data subjects could use in order to enforce their rights with regard to access to telecommunication data by police and other agencies. Moreover the personal data protection authority does not have the powers to control operations of special services with regard to data processing.
			para 56	As for the question of whether the interference caused by Directive 2006/24 is limited to what is strictly necessary, it should be observed that, in accordance with Article 3 read in conjunction with Article 5(1) of that directive, the directive requires the retention of all traffic data concerning fixed telephony, mobile telephony, Internet access, Internet e-mail and Internet telephony. It therefore applies to all means of electronic communication, the use of which is very widespread and of growing importance in people's everyday lives. Furthermore, in accordance with Article3 of Directive 2006/24, the directive covers all subscribers and registered users. It therefore entails an interference with the fundamental rights of practically the entire European population.	Polish law does not provide division between different categories of individual. Telecommunication operators are required to gather all data generated in the territory of Poland.
			para 58	Directive 2006/24 affects, in a comprehensive manner, all persons using electronic communications services, but	National provisions do not provide for any such

				without the persons whose data are retained being, even indirectly, in a situation which is liable to give rise to criminal prosecutions. It therefore applies even to persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious crime. Furthermore, it does not provide for any exception, with the result that it applies even to persons whose communications are subject, according to rules of national law, to the obligation of professional secrecy.	differentiation.
			para 59	Moreover, whilst seeking to contribute to the fight against serious crime, Directive 2006/24 does not require any relationship between the data whose retention is provided for and a threat to public security and, in particular, it is not restricted to a retention in relation (i) to data pertaining to a particular time period and/or a particular geographical zone and/or to a circle of particular persons likely to be involved, in one way or another, in a serious crime, or (ii) to persons who could, for other reasons, contribute, by the retention of their data, to the prevention, detection or prosecution of serious offences.	The Polish provisions are similarly deficient.
			para 60	Secondly, not only is there a general absence of limits in Directive 2006/24 but Directive 2006/24 also fails to lay down any objective criterion by which to determine the limits of the access of the competent national authorities to the data and their subsequent use for the purposes of prevention, detection or criminal prosecutions concerning	Law provisions lay down criteria by which the limits of the access to data should be determined (when other measures have proved ineffective or will be inadequate), but there is no

				offences that, in view of the extent and seriousness of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter, may be considered to be sufficiently serious to justify such an interference. On the contrary, Directive 2006/24 simply refers, in Article 1(1), in a general manner to serious crime, as defined by each Member State in its national law.	authority that verifies that those criteria are met.
			para 61	Furthermore, Directive 2006/24 does not contain substantive and procedural conditions relating to the access of the competent national authorities to the data and to their subsequent use. Article 4 of the directive, which governs the access of those authorities to the data retained, does not expressly provide that that access and the subsequent use of the data in question must be strictly restricted to the purpose of preventing and detecting precisely defined serious offences or of conducting criminal prosecutions relating thereto; it merely provides that each Member State is to define the procedures to be followed and the conditions to be fulfilled in order to gain access to the retained data in accordance with necessity and proportionality requirements.	The Polish provisions are similarly deficient
			para 62	In particular, Directive 2006/24 does not lay down any objective criterion by which the number of persons authorised to access and subsequently use the data retained is limited to what is strictly necessary in the light of the objective pursued. Above all, the access by the competent national authorities to the data retained is not made dependent on a prior review carried out by a court	There is no independent body overseeing data requests. It may be worth noting, however, that the Polish Constitutional Court ruled that uncontrolled access to telecommunication data by police and other agencies is

				or by an independent administrative body whose decision seeks to limit access to the data and their use to what is strictly necessary for the purpose of attaining the objective pursued and which intervenes following a reasoned request of those authorities submitted within the framework of procedures of prevention, detection or criminal prosecutions. Nor does it lay down a specific obligation on Member States designed to establish such limits.	unconstitutional. Court ruling enters in to force in February 2016, therefore Polish government has to prepare new regulation establishing a supervisory authority and criteria by which that authority will be reviewing data access requests.
			para 63	Thirdly, so far as concerns the data retention period, Article 6 of Directive 2006/24 requires that those data be retained for a period of at least six months, without any distinction being made between the categories of data set out in Article 5 of that directive on the basis of their possible usefulness for the purposes of the objective pursued or according to the persons concerned.	National provisions do not provide for distinctions between different categories of data. After the Data Retention Directive was implemented, all types of data had to be retained for 24 months. The law has been changed a couple of years later and now telecommunication data are retained for 12 months.
			para 64	Furthermore, that period is set at between a minimum of 6 months and a maximum of 24 months, but it is not stated that the determination of the period of retention must be based on objective criteria in order to ensure that it is limited to what is strictly necessary.	National provisions do not base the determination of the length of the retention period on objective criteria. After the end of the retention period data telecommunication operators are required to destroy data.
			para 65	It follows from the above that Directive 2006/24 does not	We are not aware of such criteria

				lay down clear and precise rules governing the extent of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter. It must therefore be held that Directive 2006/24 entails a wide-ranging and particularly serious interference with those fundamental rights in the legal order of the EU, without such an interference being precisely circumscribed by provisions to ensure that it is actually limited to what is strictly necessary.	being adopted or applied by Polish authorities.
			para 66	Moreover, as far as concerns the rules relating to the security and protection of data retained by providers of publicly available electronic communications services or of public communications networks, it must be held that Directive 2006/24 does not provide for sufficient safeguards, as required by Article 8 of the Charter, to ensure effective protection of the data retained against the risk of abuse and against any unlawful access and use of that data. In the first place, Article 7 of Directive 2006/24 does not lay down rules which are specific and adapted to (i) the vast quantity of data whose retention is required by that directive, (ii) the sensitive nature of that data and (iii) the risk of unlawful access to that data, rules which would serve, in particular, to govern the protection and security of the data in question in a clear and strict manner in order to ensure their full integrity and confidentiality. Furthermore, a specific obligation on Member States to establish such rules has also not been laid down.	Telecommunication operators are required to protect retained data, ensuring its integrity, quality and the sensitive nature of data. Retained data is protected under the telecommunication communications confidentiality regime and operators are required to limit access to data only to authorized personnel.

			para 67	Article 7 of Directive 2006/24, read in conjunction with Article 4(1) of Directive 2002/58 and the second sub-paragraph of Article 17(1) of Directive 95/46, does not ensure that a particularly high level of protection and security is applied by those providers by means of technical and organisational measures, but permits those providers in particular to have regard to economic considerations when determining the level of security which they apply, as regards the costs of implementing security measures. In particular, Directive 2006/24 does not ensure the irreversible destruction of the data at the end of the data retention period.	Retained telecommunication data are protected under the communication confidentiality regime.
			para 68	In the second place, it should be added that that directive does not require the data in question to be retained within the European Union, with the result that it cannot be held that the control, explicitly required by Article 8(3) of the Charter, by an independent authority of compliance with the requirements of protection and security, as referred to in the two previous paragraphs, is fully ensured. Such a control, carried out on the basis of EU law, is an essential component of the protection of individuals with regard to the processing of personal data (see, to that effect, Case C-614/10 Commission v Austria EU:C:2012:631, paragraph 37).	National provisions do not expressly require that data must be retained within the EU.
			para 69	Having regard to all the foregoing considerations, it must be held that, by adopting Directive 2006/24, the EU legislature has exceeded the limits imposed by compliance with the principle of proportionality in the	National provisions on data retention and access to telecommunication data exceed limits imposed by compliance

				light of Articles 7, 8 and 52(1) of the Charter.	with the principle of proportionality. It is also noteworthy that Polish Constitutional Court ruling stated that uncontrolled access to retained data is unconstitutional.
United Kingdom	Data retention and Investigatory Powers Act (DRIPA), 2014 Regulation of Investigatory Powers Act (RIPA), 2000	Section 1 and Section 37	para 58	Directive 2006/24 affects, in a comprehensive manner, all persons using electronic communications services, but without the persons whose data are retained being, even indirectly, in a situation which is liable to give rise to criminal prosecutions. It therefore applies even to persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious crime. Furthermore, it does not provide for any exception, with the result that it applies even to persons whose communications are subject, according to rules of national law, to the obligation of professional secrecy.	DRIPA fails to specify restrictions on the Secretary of State's entitlement to issue a retention notice. There is nothing in the provisions that requires a retention notice to exclude persons whose communications are subject to professional secrecy obligations, with the exception of the recently added safeguards related to the access to data of journalists.[v] The retention notice is likely to cover the data of persons for whom there is no evidence suggesting their conduct might have a link, even an indirect or remote one, with a serious crime.
			para 59	Moreover, whilst seeking to contribute to the fight	There is no requirement that there

				against serious crime, Directive 2006/24 does not require any relationship between the data whose retention is provided for and a threat to public security and, in particular, it is not restricted to a retention in relation (i) to data pertaining to a particular time period and/or a particular geographical zone and/or to a circle of particular persons likely to be involved, in one way or another, in a serious crime, or (ii) to persons who could, for other reasons, contribute, by the retention of their data, to the prevention, detection or prosecution of serious offences.	is any relationship between the person whose data is being collected and a situation that is liable to give rise to criminal prosecutions or a threat to public security.
			para 61	Furthermore, Directive 2006/24 does not contain substantive and procedural conditions relating to the access of the competent national authorities to the data and to their subsequent use. Article 4 of the directive, which governs the access of those authorities to the data retained, does not expressly provide that that access and the subsequent use of the data in question must be strictly restricted to the purpose of preventing and detecting precisely defined serious offences or of conducting criminal prosecutions relating thereto; it merely provides that each Member State is to define the procedures to be followed and the conditions to be fulfilled in order to gain access to the retained data in accordance with necessity and proportionality requirements.	Access to the data is not restricted to uses relating to precisely defined serious offences. The data may be accessed for broad purposes, including national security, preventing and detecting crime, economic well-being related to national security public safety, public health, tax collection and preventing death or injury. This has occurred, for example, in cases concerning filesharers or in defamation cases.[vi] Furthermore section 37 of the Protection of Freedoms Act 2012 introduced a requirement for prior judicial authorisation for

					access to communications data by local authorities (councils). These just constitute under 1% of all access.[vii]
			para 62	In particular, Directive 2006/24 does not lay down any objective criterion by which the number of persons authorised to access and subsequently use the data retained is limited to what is strictly necessary in the light of the objective pursued. Above all, the access by the competent national authorities to the data retained is not made dependent on a prior review carried out by a court or by an independent administrative body whose decision seeks to limit access to the data and their use to what is strictly necessary for the purpose of attaining the objective pursued and which intervenes following a reasoned request of those authorities submitted within the framework of procedures of prevention, detection or criminal prosecutions. Nor does it lay down a specific obligation on Member States designed to establish such limits.	In some cases retained data can be accessed through a court order or other judicial authorisation or warrant. But, for the most part, government or other public officials can access the data directly without the need for judicial authorisation, in accordance with the Regulation of Investigatory Powers Act (RIPA).
			para 68	In the second place, it should be added that that directive does not require the data in question to be retained within the European Union, with the result that it cannot be held that the control, explicitly required by Article 8(3) of the Charter, by an independent authority of compliance with the requirements of protection and security, as referred to	There is no requirement that the data is retained within the EU.

				in the two previous paragraphs, is fully ensured. Such a control, carried out on the basis of EU law, is an essential component of the protection of individuals with regard to the processing of personal data (see, to that effect, Case C-614/10 Commission v Austria EU:C:2012:631, paragraph 37).	

i See 3.2.4.1 and 3.2.4.3 in ”Notat om betydningen af EU-Domstolens dom af 8. april 2014 i de forenede sager C-293/12 og C-594/12 (om logningsdirektivet) for de danske logningsregler”, Ministry of Justice, 2 June 2014 (legal analysis of the CJEU data retention ruling) http://justitsministeriet.dk/sites/default/files/media/Pressemeddelelser/pdf/2014/Notat%20om%20logningsdirektivet.pdf

ii See 3.2.4.2 in ”Notat om betydningen af EU-Domstolens dom af 8. april 2014 i de forenede sager C-293/12 og C-594/12 (om logningsdirektivet) for de danske logningsregler”, Ministry of Justice, 2 June 2014.

iii Administration of Justice Act, Section 783(1) and 783(4).

iv Johanna Niemi & Virve-Maria de Godzinsky: *Telepakkokeinojen oikeussuojajärjestelmä*. Oikeuspoliittisen tutkimuslaitoksen tutkimuksia 243. Helsinki 2009.

v https://www.gov.uk/government/publications/communications-data-draft-codes-of-practice-acquisition-disclosure-and-retention

vi http://www.2tg.co.uk/assets/docs/newsletter_documents/a_practical_guide_to_norwich_pharmacal_orders_-_spring_2014.pdf

vii https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/225120/isc-access-communications.pdf