

National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies

DENMARK

Version of 17 September 2014

Danish Institute for Human Rights
Anja Møller Pedersen and
Rikke Frank Jørgensen

DISCLAIMER: This document was commissioned under a specific contract as background material for the project on [National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies](#). The information and views contained in the document do not necessarily reflect the views or the official position of the EU Agency for Fundamental Rights. The document is made publicly available for transparency and information purposes only and does not constitute legal advice or legal opinion. FRA would like to express its appreciation for the comments on the draft report provided by Denmark that were channelled through the FRA National Liaison Officer.

Summary

1 Surveillance legal framework in Denmark

1.1 The Danish Security and Intelligence Service (*Politiets Efterretningstjeneste (PET)*)

- [1]. PET is the Danish national security and intelligence service and a part of the Danish National Police.¹ PET works to identify, prevent and counter threats to freedom, democracy and security in Denmark as well as threats directed at Danish nationals and Danish interests abroad,² including threats as defined in Chapter 12 and 13 of the Danish Penal Code e.g. terrorism, extremism and espionage.³ On 1 January 2014 a new act codifying the activities of PET entered into force.⁴ While not altering the basic tasks of PET, it established new rules on how to collect, process and disclose personal data.
- [2]. The term “mass surveillance” does not exist in the Danish legal framework and is not connected with the possibilities in the Danish Administration of Justice Act (*retsplejeloven*) for carrying out coercive measures. PET collects information that “could be of importance” to its activities and conducts investigations e.g. observation of individuals/undertakings that “can be assumed to be of importance” to its efforts in relation to counter-terrorism or that are “strictly required” to its other activities. Investigative and coercive measures must be conducted in accordance with the Danish Administration of Justice Act.⁵ A prior court order is required, except in urgent cases, and there must be grounds for suspicion of certain “serious crimes”. However, observation in open space or without use of optical devices does not require a court order. Furthermore, public authorities are obligated to pass on to PET information that “could be of importance” to PET’s activities in relation to counter-terrorism etc.
- [3]. The activities of PET are exempted from the Danish Public Information Act,⁶ parts of the Danish Public Administration Act⁷ and the Danish Act on Processing of Personal Data.⁸

2

¹ Denmark, Report no. 1529/2012 of the Expert Committee on the Danish Security and Intelligence Service and the Danish Defence Intelligence Service (*Betænkning nr. 1529/2012 om PET og FE*), February 2012, available in Danish at http://www.statensnet.dk/betaenkninger/1401-1600/1529-2012/1529-2012_pdf/printversion_1529-2012.pdf.

² The Danish Security and Intelligence Service (*Politiets Efterretningstjeneste (PET)*), information available in English at: <https://www.pet.dk/English/About%20PET.aspx>.

³ Denmark, The Danish Penal Code, Consolidated act no. 871 of 4 July 2014 (*Straffeloven, lovbekendtgørelse nr. 871 af 4. juli 2014*), available in Danish at: <https://www.retsinformation.dk/Forms/R0710.aspx?id=164192>.

⁴ Denmark, Act no. 604 of 12 June 2013 on the Danish Security and Intelligence Service as amended by Act. no. 1624 of 26 December 2013 (*Lov nr. 604 af 12. juni 2013 om Politiets Efterretningstjeneste (PET), som ændret ved lov nr. 1624 af 26. december 2013*), available in Danish at: <https://www.retsinformation.dk/Forms/R0710.aspx?id=152182>.

⁵ Denmark, The Danish Administration of Justice Act, Consolidated act no. 1139 of 24 September 2013, (*Retsplejeloven, lovbekendtgørelse nr. 1139 af 24. september 2013*), book no. 4, second paragraph, available in Danish at: <https://www.retsinformation.dk/Forms/R0710.aspx?id=157953>.

⁶ Denmark, The Danish Public Information Act, Act no. 606 of 12 June 2013 (*Offentlighedsloven, lov nr. 606 af 12. juni 2013*), available in Danish at: <https://www.retsinformation.dk/Forms/R0710.aspx?id=152299>.

⁷ Denmark, The Danish Public Administration Act, Consolidated Act no. 433 of 22 April 2014 (*Forvaltningsloven, lovbekendtgørelse nr. 433 af 22. april 2014*), available in Danish at: <https://www.retsinformation.dk/Forms/R0710.aspx?id=161411>.

⁸ Denmark, Act no. 429 of 31 May 2000 on Processing of Personal Data with later amendments (*Lov nr. 429 af 31. maj 2000 om behandling af personoplysninger med senere ændringer*), available in Danish at: www.retsinformation.dk/Forms/R0710.aspx?id=828.

2

However, the conditions set for PET's processing of information are largely based on the standards of the latter. In some instances, such as in relation to counter-terrorism, the PET act has eased the access to information from cases where this is "strictly required" to where it is "assumed to be of importance". Information is, as a general rule, to be deleted after 15 years.

1.1.1 The Danish Defence Intelligence Service (DDIS) (*Forsvarets Efterretningstjeneste (FE)*)

- [4]. On 1 January 2014 a new act codifying the activities of DDIS entered into force.⁹ DDIS is Denmark's foreign and military intelligence service. It collects, analyses, and disseminates information about conditions abroad of importance to Denmark's security, e.g. information of political, financial, scientific, and military interest, international terrorism, extremists etc. Information that "could be of importance" to the activities of PET can be passed on to PET.
- [5]. The activities of DDIS are exempted from the Public Information Act, parts of the Public Administration Act and the Act on Processing of Personal Data, and the conditions for access to information are largely similar to the PET-Act.

1.1.2 The Danish Centre for Cyber Security (CfCS) (*Center for Cybersikkerhed*)

- [6]. CfCS is Denmark's national ICT security authority and has the responsibility to contribute to protect and warn against cyber threats/attacks, counter cyber-attacks and handle the warning services – CERTs (Computer Emergency Response Team) - MILCERT (military) and GovCERT (civil).¹⁰ The activities of CfCS are regulated in the CfCS Act¹¹ that placed CfCS within DDIS and exempted its activities from the Public Information Act, parts of the Public Administration Act and the Act on Processing of Personal Data, which has led to critique and concern about the exchange of information with DDIS and other authorities.¹²
- [7]. State bodies/authorities, regions, municipalities and undertakings with functions of social importance can request connection to the ICT security service and GovCERT thus monitors the activities on their connections to external networks, including the internet. Without court order, CfCS collects data transmitted through the digital networks and traffic data.
- [8]. The processing of personal data is allowed, only by consent or if "strictly required" to the activities of CfCS. In case of well-founded suspicion of a security threat, transmitted data can be analysed and passed on to the police, and if strictly required to the activities of CfCS, moreover, it can be passed on to other authorities and similar warning services in Denmark and abroad.¹³ Data shall be deleted when the purpose of the processing is fulfilled, and within 3 years at latest (in relation to a security threat).

⁹ Denmark, Act no. 602 of 12 June 2013 on the Danish Defence Intelligence Service (*Lov nr. 602 af 12. juni 2013 om Forsvarets Efterretningstjeneste (FE)*), available in Danish at: www.retsinformation.dk/Forms/r0710.aspx?id=152195.

¹⁰ The Danish Centre for Cyber Security (*Center for Cybersikkerhed*), information available in Danish at: <http://fe-ddis.dk/cfcs/Pages/cfcs.aspx>.

¹¹ Denmark, Act. no. 713 of 25 June 2014 on the Danish Centre for Cyber Security (*lov nr. 713 af 25. juni 2014 om Center for Cybersikkerhed*), available in Danish at: <https://www.retsinformation.dk/Forms/R0710.aspx?id=163853>.

¹² Danish Institute for Human Rights (*Institut for Menneskerettigheder*) (2014), "*Høring over udkast til forslag til lov om Center for Cybersikkerhed samt evaluering af GovCERT-loven, j.nr. 540.10/30403/RFJ/MAF*", 4 March 2014, available in Danish at: http://menneskeret.dk/files/media/hoeringssvar/hoeringssvar_afgivet_i_2014/marts%202014/marts_2014_tilgaengeligt/24_b_center_for_cybersikkerhed.pdf.

¹³ Denmark, Bill no. 192 of 8 May 2014 on the Act on the Danish Centre for Cyber Security (*Lovforslag nr. 192 af 8. maj 2014 om Center for Cybersikkerhed*), available in Danish at: <https://www.retsinformation.dk/Forms/R0710.aspx?id=162037>.

1.1.3 The Danish Administration of Justice Act and Administrative Order on Data Retention

- [9]. According to the Danish Administration of Justice Act¹⁴ and the Administrative Order on Data Retention,¹⁵ all providers of electronic communication services or networks shall retain data generated or processed by the network of the provider for the purpose of potential investigation of criminal matters. Data is accessed in accordance with the Administration of Justice Act,¹⁶ cf. the above, and is retained for one year. The regulation is largely equivalent to Directive 2006/24/EC on Data Retention.
- [10]. Critique has been raised that the data retention rules did not seem necessary and proportionate in a democratic society.¹⁷ Following the invalidation of Directive 2006/24/EC by the Court of Justice of the European Union, the Danish Government on 2 June 2014 presented a legal analysis on the implications for the Danish Data Retention rules.¹⁸ The analysis concluded that in general the Danish data retention law is not affected by the CJEU ruling, The Minister of Justice did, however, lift the requirement on internet session logging with immediate effect a.o. due to technical difficulties of using the retained data on internet sessions for police investigations. Moreover, the Minister of Justice has announced that the data retention law will be subject to a general evaluation in the parliamentary assembly 2014/15.¹⁹

1.2 Safeguards put in place by the legal framework

1.2.1 The Danish Constitution (*Grundloven*)

- [11]. The Danish Constitution²⁰ contains two provisions related to privacy. Article 71 states that personal liberty is inviolable. Article 72 states that the dwelling is inviolable and that house search, seizure, and examination of letters and other papers, or any breach of the secrecy that shall be observed in postal, telegraph, and telephone matters, shall not take place except under a judicial order, unless particular exception is warranted by statute.

4

¹⁴ Denmark, The Danish Administration of Justice Act, Consolidated act no. 1139 of 24 September 2013, (*Retsplejeloven, lovbekendtgørelse nr. 1139 af 24. september 2013*), Section 786, available in Danish at: <https://www.retsinformation.dk/Forms/R0710.aspx?id=157953>.

¹⁵ Denmark, Administrative Order no. 988 of 28 September 2006 on Data Retention as amended by Administrative Order no. 660 of 19 June 2014 (*Logningsbekendtgørelsen, bekendtgørelse nr. 988 af 28. september 2006, som ændret ved bekendtgørelse nr. 660 af 19. juni 2014*), available in Danish at: <https://www.retsinformation.dk/Forms/R0710.aspx?id=2445>.

¹⁶ Denmark, The Danish Administration of Justice Act, Consolidated act no. 1139 of 24 September 2013, (*Retsplejeloven, lovbekendtgørelse nr. 1139 af 24. september 2013*), book no. 4, second paragraph, available in Danish at: <https://www.retsinformation.dk/Forms/R0710.aspx?id=157953>

¹⁷ Denmark, Ministry of Justice (*Justitsministeriet*), "*Oversigt over Høringssvar*", 14 December 2011, available in Danish at: http://webarkiv.ft.dk/img20012/udvibilag/lib9/20012_1119.pdf.

¹⁸ Denmark, Ministry of Justice (*Justitsministeriet*) (2014), "*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*", 2 June 2014, available in Danish at: <http://justitsministeriet.dk/sites/default/files/media/Pressemeddelelser/pdf/2014/Notat%20om%20logningsdirektivet.pdf>.

¹⁹ Denmark, Ministry of Justice (*Justitsministeriet*) (2014), "Justitsministeren ophæver reglerne om sessionslogging", Press release, 2 June 2014, information available in Danish at: <http://www.justitsministeriet.dk/nyt-og-presse/pressemeddelelser/2014/justitsministeren-oph%C3%A6ver-reglerne-om-sessionslogging>.

²⁰ Denmark, The Danish Constitutional Act, Act. no. 169 of 5 June 1953 (*Grundloven, Lov nr. 169 af 5. juni 1953*), available in Danish at: <https://www.retsinformation.dk/Forms/R0710.aspx?id=45902>, available in English at: <http://www.eu-oplysningen.dk/upload/application/pdf/0172b719/Constitution%20of%20Denmark.pdf>.

4

1.2.2 The Danish Act on the Processing of Personal Data (*Persondataloven*) and The Danish Data Protection Agency (*Datatilsynet*)

- [12]. The Act on Processing of Personal Data²¹ implements Directive 95/46/EC on the protection of processing of personal data. It sets the boundaries for how public authorities and private companies must process collected personal data on citizens and customers.
- [13]. The Danish Data Protection Agency monitors the observance of the act ex officio (decision making and inspections) or by complaint. In 2013 the Agency registered 6,118 new cases.²² However, as the activities of PET, DDIS and CfCS have been exempted from the Act on the Processing of Data, and the Data Protection Agency has no authority in relation to their activities. Furthermore, the Data Protection Agency has no authority in relation to the Data Retention rules.

1.2.3 The Oversight Committee of PET and DDIS (*Tilsynet med Efterretningstjenesterne*)

- [14]. The PET and DDIS Acts introduced the establishment of The Oversight Committee of PET and DDIS whose main objective is to ensure – either ex officio or by complaint – the observance by PET and DDIS, including CfCS, of the rules on access to personal data, but not the rules on investigative and coercive measures.

1.2.4 The Parliamentary Control Committee (*Folketingets udvalg vedrørende efterretningstjenestene, “Kontroludvalget”*)

- [15]. The Parliamentary Control Committee is established to gain insight into PET and DDIS.²³ On 1 January 2014 a new act to strengthen its work entered into force.²⁴ It obligates the Government to provide the Committee with an annual briefing on the activities of PET and DDIS, including PET’ use of agents and coercive measures not approved by court.²⁵ However, due to confidentiality of the members, the recommendations of the Committee are not public.
- [16]. As the control mechanisms in relation to PET and DDIS focus primarily on the processing of personal data and lack focus on the remaining activities of the services, critique has been raised, stressing that the control mechanisms are too weak.²⁶ Currently the possibility of a whistle-

5

²¹ Denmark, Act no. 429 of 31 May 2000 on Processing Personal Data with amendments (*Lov nr. 429 af 31. maj 2000 om behandling af personoplysninger med senere ændringer*), available in Danish at: www.retsinformation.dk/Forms/R0710.aspx?id=828, available in English at: <http://www.datatilsynet.dk/english/the-act-on-processing-of-personal-data/read-the-act-on-processing-of-personal-data/compiled-version-of-the-act-on-processing-of-personal-data/>.

²² Denmark, Data Protection Agency (*Datatilsynet*) (2014), Annual report 2013, available in Danish at: http://www.datatilsynet.dk/fileadmin/user_upload/dokumenter/AArsberetninger/Datatilsynets_aarsrapport_-_underskrevet.pdf.

²³ Denmark, Act no. 378 of 6 July 1988 on the establishment of a committee on the Danish Defence Intelligence Service and the Danish Security and Intelligence Service as amended by Act no. 632 of 12 June 2013 (*Lov nr. 378 af 6. juli 1988 som ændret ved lov nr. 632 af 12. juni 2013*), available in Danish at: <https://www.retsinformation.dk/Forms/R0710.aspx?id=59424>.

²⁴ Denmark, Act no. 632 of 12 June 2013 amending the Act on establishing a committee on the Danish Security and Intelligence Service and the Danish Defence Intelligence Service (*Lov nr. 632 af 12. juni 2013 om ændring af lov om etablering af et udvalg om forsvarets og politiets efterretningstjenester*), available in Danish at: www.retsinformation.dk/Forms/r0710.aspx?id=152183.

²⁵ Denmark, Bill no. 162 of 27 February 2013, amending the Act no. 378 of 6 July 1988 on the establishment of a committee on the Danish Defence intelligence Agency and the Danish Security and Intelligence Service (*Lovforslag nr. 162 af 27. februar 2013 om ændring af lov nr. 378 af 6. juli 1988 om etablering af et udvalg om forsvarets og politiets efterretningstjenester*), available in Danish at: <https://www.retsinformation.dk/Forms/R0710.aspx?id=145508>.

²⁶ Danish Institute for Human Rights (*Institut for Menneskerettigheder*) (2013), 'Høring over betænkning nr. 1592/2012 om PET og FE', j. no. 540.10/27157/PVK/ SWG/RFJ/HSC, 8 June 2012,

blower mechanism available for the staff at PET and DDIS is being discussed.²⁷ Furthermore the Danish Liberal Party (*Venstre*) has suggested, that the citizens should be made aware when they are being subject to surveillance by the State.²⁸ Finally, the Government has just suggested to appoint a commission to review the Danish legislation adopted following 11 September 2001 with a view to secure the rule of law.²⁹ This has been suggested by the Danish Institute for Human Rights since 2011.

1.3 Judicial and non-judicial remedies available to an individual

1.3.1 PET and DDIS, including CfCS

- [17]. Individuals/undertakings are not, as a general rule, allowed insight in potential processing by PET/DDIS in information about them. However, individuals/undertakings can file a complaint to the Oversight Committee of PET and DDIS which can lead to – in extraordinary cases – partly or full insight in the information. Furthermore, individuals/undertakings can request the Oversight Committee to examine whether wrongful processing of information about them is being conducted. The plaintiff will not gain knowledge of whether this is or has been the case, but the Oversight Committee shall assure that wrongful processing is ceased.
- [18]. Furthermore, investigative and coercive measures, shall be conducted in accordance with the Administration of Justice Act cf. the above. As a main rule, subjects to coercive measures shall be informed when the measure is terminated.
- [19]. Finally, the activities of PET, both in relation to general administration and decision-making, are considered subject to the general judicial control according to Section 63 of the Danish Constitution, if the ordinary judicial conditions (*locus standi*) are met. Likewise, the activities and decisions of the Oversight Committee are subject to ordinary judicial control according to Section 63 of the Constitution.³⁰ According to Section 63 the courts of justice shall be empowered to decide any question relating to the scope of the executive's authority i.e.

6

available in Danish at:

http://menneskeret.dk/files/media/hoeringssvar/hoeringssvar_afgivet_i_2012/juni_2012/50_b_betaenkning_om_pet_og_fe.pdf, Berlingske (2012), "PET-lov risikerer at blive en papirtiger" by Jonas Christoffersen and Louise Holck, 22. september 2012, available in Danish at:

<http://www.b.dk/kronikker/pet-lov-risikerer-at-blive-en-papirtiger> and The Danish Institute for Human Rights (*Institut for Menneskerettigheder*) (2013), 'Høring over udkast til forslag til lov om ændring af lov om etablering af et udvalg om forsvarets og politiets efterretningstjenester (styrkelse af den parlamentariske kontrol og indsigt)', j. no.540.10/28538/HSC/JCH, 11 February 2013, available in Danish at:

http://menneskeret.dk/files/media/hoeringssvar/h%C3%B8ringssvar_afgivet_i_2013/februar_2013/24_b_styrkelse_af_kontroludvalget.pdf.

²⁷ Berlingske (2014), "SF vil styrke tilsynet med PET og FE", 21 July 2014, available in Danish at: <http://www.b.dk/politiko/sf-vil-styrke-tilsynet-med-pet-og-fe>.

²⁸ Berlingske (2014), "Vestre: Du skal have besked, når det offentlige lurer på dig", 30 July 2014, available in Danish at: <http://www.b.dk/politiko/venstre-du-skal-have-besked-naar-det-offentlige-lurer-paa-dig>.

²⁹ Berlingske (2014), "Bred enighed: Ny terrorkommission skal være bredt sammensat", 12 August 2014, available in Danish at: <http://www.b.dk/politiko/bred-enighed-ny-terrorkommission-skal-vaere-bredt-sammensat>.

³⁰ Denmark, Report no. 1529/2012 of the Expert Committee on the Danish Security and Intelligence Service and the Danish Defence Intelligence Service (*Betænkning nr. 1529/2012 om PET og FE*), February 2012, available in Danish at http://www.statensnet.dk/betaenkninger/1401-1600/1529-2012/1529-2012_pdf/printversion_1529-2012.pdf, and Denmark, Bill no. 163 of 27 February 2013 on the Danish Defence Intelligence Service, (Lovforslag nr. 163 af 27. februar 2013 om Forsvarets Efterretningstjeneste (FE)), available in Danish at: <https://www.retsinformation.dk/Forms/R0710.aspx?id=145518>.

6

administrative acts and decisions. However, the courts of justice examine only the executive's application of law (*forvaltningens retsanvendelse*), not its discretionary assessment (*forvaltningens skøn*). This means that the courts of justice are entitled to challenge the application of law in question, but to the extent that such law contains discretionary powers for the executive, the courts are entitled to challenge only the limits of such powers, not the discretionary assessment therein. The relatively large margin of discretion held by the intelligence services, and in fact also the Oversight Committee, particularly in relation to the right to insight in the activities of the intelligence services, must therefore be taken into account when estimating the potential effect of a claim under Section 63.

- [20]. Furthermore, as mentioned above, the use of coercive measures is subject to prior judicial control by the requirement of a court order.

1.4 Annex 1 – Legal Framework relating to mass surveillance

A- Details on legal basis providing for mass surveillance

Name and type of the mass surveillance-related law	A definition of the categories of individuals liable to be subjected to such surveillance	Nature of circumstances which may give rise to surveillance	List purposes for which surveillance can be carried out	Previous approval / need for a warrant	List key steps to be followed in the course of surveillance	Time limits, geographical scope and other limits of mass surveillance as provided for by the law	Is the law allowing for mass surveillance in another country (EU MS or third countries)?
<i>Full name in English and national languages indicating its type – Act of the parliament, Government order, etc.</i>			<i>National security, economic well-being, etc....</i>	<i>Indicate whether any prior/ex post judicial warrant or a similar permission is needed to undertake surveillance and whether such approval/warrant needs to be regularly reviewed</i>	<i>See for example the principles developed by the European Court of Human Rights in the case of Weber and Saravia v. Germany, (dec.) n°54934/00, 29 June 2006, para. 95 Steps could include collecting data, analysing data, storing data, destroying data, etc.</i>	<i>Clearly state if there are any existing limitations in terms of nationality, national borders, time limits, the amount of data flow caught etc.</i>	<i>Please, provide details</i>
Denmark, the Danish Administration of Justice Act, Consolidated act no. 1139 of 24	Regulates the use of <u>coercive and investigative measures</u> .	1) Specific grounds for suspicion that information is being transferred	Please see the previous column.	A prior court order is required, except in urgent cases. Under such circumstances, within 24 hours	Regulates only the use of coercive and investigative measures.	<u>Geographical scope</u> : Court orders shall be obtained in accordance with Danish rules of	Please see the previous column.

<p>September 2013, (<i>Retsplejeloven, lovbekendtgørelse nr. 1139 af 24. september 2013</i>).</p> <p>The term “mass surveillance” does not exist in the Danish legal framework and is not connected with the possibilities in the Danish Administration of Justice Act (<i>retsplejeloven</i>) for carrying out coercive measures.</p>	<p>Individuals/undertakings liable to such measures are:</p> <ol style="list-style-type: none"> 1) Suspects 2) Subordinates, 3) Potential victims of terrorism etc. 4) Others whose activities form part of background knowledge of the social order. 	<p>from/to the subject of the coercive measure,</p> <ol style="list-style-type: none"> 2) The coercive measure is strictly required to the investigation, <u>and</u> 3) Investigation is conducted in relation to all crimes liable to a minimum of 6 years of imprisonment or certain serious crimes in relation to Chapter 12 and 13 of the Danish Penal Code e.g. terrorism and other provisions in the Danish Penal Code. 		<p>from the execution of the coercive measure, the decision must be introduced before court and thus approved (<i>forelagt retten til prøvelse</i>).</p> <p>The court order must indicate a time limit – as short as possible and a maximum of 4 weeks (can be prolonged by new court orders)</p>		<p>jurisdiction of the district courts.</p> <p>The act does not contain further rules on jurisdiction. Reference is thus made to the ordinary principles of jurisdiction according to public international law as described in Articles 6 – 12 in the Danish Penal Code.</p>	
--	---	---	--	---	--	--	--

<p>Denmark, Act no. 604 of 12 June 2013 on the Danish Security and Intelligence Service as amended by Act. no. 1624 of 26 December 2013 (<i>Lov nr. 604 af 12. juni 2013 om Politiets Efterretningstjeneste (PET) som ændret ved lov nr. 1624 af 26. december 2013</i>)</p>	<p>Please see the above column.</p>	<p>PET collects information that “could be of importance” to its activities, cf. Article 3.</p> <p>Furthermore, public authorities are obligated to pass on to PET information that “could be of importance” to PET’s activities in relation to counter-terrorism etc., cf. Article 4</p> <p>PET conducts investigations e.g. observation of individuals/undertakings that “can be assumed to be of importance” to its efforts in relation to counter-terrorism or that</p>	<p>Threats, incl. terrorism, to freedom, democracy and safety in Denmark as well as threats directed at Danish nationals and Danish interests abroad, cf. Article 1.</p>	<p>Coercive and investigative measures shall be conducted in accordance with the Administration on Justice Act, cf. the above, cf. Article 6.</p>	<p>Collecting, analysing, storing and destroying data.</p>	<p>The <u>geographical scope</u> of the act is not indicated. However, PET works to prevent and investigate threats in Denmark as well as threats directed at Danish nationals/ interests abroad.</p> <p>Reference is thus made to the ordinary principles of jurisdiction according to public international law as described in Articles 6 – 12 in the Danish Penal Code.</p>	<p>Please see the previous column.</p>
---	-------------------------------------	---	--	---	--	--	--

		<p>are “strictly required” to its other activities, cf. Article 5.</p> <p>Coercive and investigative measures shall be conducted in accordance with the Administration of Justice Act, cf. the above, cf. Article 6.</p>					
<p>Denmark, Act no. 602 of 12 June 2013 on the Danish Defence Intelligence Service (DDIS) (<i>Lov nr. 602 af 12. juni 2013 om Forsvarets Efterretningstjeneste (FE)</i>)</p>	<p>DDIS collects information about circumstances <u>abroad</u> of importance to the Danish Foreign, Security and Defence Policy, e.g. military, political, economic, transnational (terrorism etc.) and technical/scientific information,</p>	<p>According to the preparatory works, DDIS uses any investigative measure available according to Danish Law. However, DDIS does not have the power to conduct coercive and investigative measures, only with the assistance of PET/the Police</p>	<p>Please see the previous columns.</p>	<p>Please see the previous columns.</p>	<p>Collection, processing, storing and destroying data.</p>	<p>The power to collect information is <u>geographical neutral</u> and not limited to Danish territory, cf. Article 1.</p>	<p>Please see the previous column.</p>

	incl. personal data, cf. Article 1.	or the Military Prosecution Service. ³¹					
Denmark, Act no. 713 of 25 June 2014 on The Danish Centre for Cyber Security (CfCS) (<i>Lov nr. 713 af 25. juni 2014 om Center for Cybersikkerhed</i>)	1) <u>Connected</u> State bodies/authorities, regions, municipalities and undertakings with social functions. in case of well-founded suspicion of a security threat: 2) <u>Temporarily connected</u> units, <u>and</u> And by request 3) <u>Other units</u>	MILCERT/Gov CERT monitor the connected networks. In accordance with Articles 4 – 7, CfCS collects/process data transmitted through the digital networks and traffic data of the <u>connected units</u> etc. cf. the previous column. The processing of personal data shall be proportionate. It is allowed only by consent or if “strictly required” to	Please see the previous columns.	No court order is required.	Monitoring, collecting, analysing, storing and destroying data.	The <u>geographical scope</u> is not indicated in the act. Reference is thus made to the ordinary principles of jurisdiction according to public international law as described in Articles 6 – 12 in the Danish Penal Code.	Please see the previous column.

³¹ Denmark, Bill no. 163 of 27 February 2013 on the Danish Defence Intelligence Service, (*Lovforslag nr. 163 af 27. februar 2013 om Forsvarets Efterretningstjeneste (FE)*), available in Danish at: <https://www.retsinformation.dk/Forms/R0710.aspx?id=145518> and Denmark, Report no. 1529/2012 of the Expert Committee on the Danish Security and Intelligence Service and the Danish Defence Intelligence Service (*Betænkning nr. 1529/2012 om PET og FE*), available in Danish at http://www.statensnet.dk/betaenkninger/1401-1600/1529-2012/1529-2012_pdf/printversion_1529-2012.pdf.

		certain activities of CfCS. ³² Analysis and the pass on to the police of data transmitted through the networks requires well-founded suspicion of a security threat, cf. Article 15 – 16.					
Denmark, The Danish Administration of Justice Act, Consolidated act no. 1139 of 24 September 2013, (<i>Retsplejeloven, lovbekendtgørelse nr. 1139 af 24. september 2013</i>), Section 786. Denmark, Administrative	All users of electronic communication.	The data retention rules are largely equivalent to Directive 2006/24/EC on Data Retention. Providers of electronic communication services or networks shall retain data generated or processed by the network of the	Please see the previous column.	The retention itself requires no court order. Data is accessed/process and passed on to the police in accordance with the Administration of Justice Act, thus a prior court order is required, cf. the above.	Retaining, potential passing on of information to the police, storing and destroying data.	The <u>geographical scope</u> is not indicated. Reference is thus made to the ordinary principles of jurisdiction according to public international law as described in Articles 6 – 12 in the Danish Penal Code.	Please see the previous column.

³² Denmark, Bill no. 192 of 8 May 2014 on the Act on the Danish Centre for Cyber Security (*Lovforslag nr. 192 af 8. Maj 2014 om Center for Cybersikkerhed*), available in Danish at: <https://www.retsinformation.dk/Forms/R0710.aspx?id=162037>.

<p>Order no. 988 of 28 September 2006 on Data Retention as amended by Administrative Order no. 660 of 19 June 2014 (<i>Logningsbeken dtgørelsen, bekendtgørelse nr. 988 af 28. september 2006, som ændret ved bekendtgørelse nr. 660 af 19. juni 2014</i>)</p>		<p>provider for the purpose of potential investigation of criminal matters.</p> <p>Data is accessed in accordance with the rules on coercive and investigative measures in in Administration of Justice Act, cf. the above.</p>					
--	--	---	--	--	--	--	--

B- Details on the law providing privacy and data protection safeguards against mass surveillance

<p>Please, list law(s) providing for the protection of privacy and data protection against unlawful surveillance</p>	<p>List specific privacy and data protection safeguards put in place by this law(s)</p>	<p>Indicate whether rules on protection of privacy and data protection apply:</p> <p>only to nationals or also to EU citizens and/or third country nationals</p>	<p>Indicate whether rules on protection of privacy and data protection apply:</p> <p>only inside the country, or also outside (including differentiation if EU or outside EU)</p>
<p><i>Include a reference to specific provision and describe their content</i></p>	<p><i>e.g. right to be informed, right to rectification/deletion/blockage, right to challenge, etc.</i></p>	<p><i>Please, provide details</i></p>	<p><i>Please, provide details</i></p>
<p>Denmark, The Danish Constitution, Act. no. 169 of 5 June 1953 (<i>Grundloven, Lov nr. 169 af 5. juni 1953</i>), Articles 71 and 72.</p>	<p>Personal liberty is inviolable, cf. Article 71. The dwelling is inviolable and that house search, seizure, and examination of letters and other papers, or any breach of the secrecy that shall be observed in postal, telegraph, and telephone matters, shall not take place except under a judicial order, unless particular exception is warranted by statute, cf. Article 72.</p>	<p>The act applies to all Danish territory, cf. Article 1. Besides Articles 71, first paragraph, second sentence (regards deprivation of liberty on the grounds of political and religious conviction), which applies only to Danish citizens, Article 71 and 72 apply to any person, Danish or foreigner, on Danish territory.</p>	<p>Please see the previous column.</p>
<p>Denmark, The Danish Administration of Justice Act, Consolidated act no. 1139 of 24 September 2013, (<i>Retsplejeloven</i>,</p>	<p>Coercive / investigative measures: Prior court order is – as a main rule – required, cf. Article 783. When terminated – as a main rule – the subject shall be informed, cf. Article 788.</p>	<p>Not regulated by the act. Reference is thus made to the ordinary principles of jurisdiction according to public international law as described in Articles 6 – 12 in the Danish Penal Code.</p>	<p>Please see the previous column.</p>

<p>Please, list law(s) providing for the protection of privacy and data protection against unlawful surveillance</p>	<p>List specific privacy and data protection safeguards put in place by this law(s)</p>	<p>Indicate whether rules on protection of privacy and data protection apply:</p> <p>only to nationals or also to EU citizens and/or third country nationals</p>	<p>Indicate whether rules on protection of privacy and data protection apply:</p> <p>only inside the country, or also outside (including differentiation if EU or outside EU)</p>
<p><i>lovbekendtgørelse nr. 1139 af 24. september 2013), book no. 4, second paragraph.</i></p>			
<p>Denmark, Act no. 604 of 12 June 2013 on the Danish Security and Intelligence Service as amended by Act. no. 1624 of 26 December 2013 (<i>Lov nr. 604 af 12. juni 2013 om Politiets Efterretningstjeneste (PET) som ændret ved lov nr. 1624 af 26. december 2013</i>)</p>	<p>Coercive / investigative measures shall be conducted in accordance with the Administration of Justice Act, cf. Article 6.</p> <p><u>Access to personal data</u> requires:</p> <ol style="list-style-type: none"> 1) consent, 2) that it is “assumed to be of importance” to PET’s counter-terrorism efforts etc. <u>or</u> 3) that it is strictly required in relation to PET’s other activities. <p><u>Right to deletion:</u> Personal data shall be deleted – as a main rule – after 15 years, when no further information in relation to the investigation has been collected etc., cf. Article 7 – 9.</p> <p><u>Right to insight:</u></p>	<p>Not regulated in the PET Act.</p> <p>Reference is thus made to the ordinary principles of jurisdiction according to public international law as described in Articles 6 – 12 in the Danish Penal Code.</p>	<p>Please see the previous column.</p>

<p>Please, list law(s) providing for the protection of privacy and data protection against unlawful surveillance</p>	<p>List specific privacy and data protection safeguards put in place by this law(s)</p>	<p>Indicate whether rules on protection of privacy and data protection apply:</p> <p>only to nationals or also to EU citizens and/or third country nationals</p>	<p>Indicate whether rules on protection of privacy and data protection apply:</p> <p>only inside the country, or also outside (including differentiation if EU or outside EU)</p>
	<p>Individuals/undertakings can file a complaint to the Oversight Committee of PET and DDIS and – under extraordinary circumstances – gain partly or full insight in information about them, cf. Article 12.</p> <p>Individuals/undertakings can ask the Oversight Committee to make sure that PET is not illegally processing personal data about them, cf. Article 13.</p> <p>Individuals/undertakings can file a complaint to the Oversight Committee to make sure that PET observes the rules on the processing of personal data set out in the PET act, cf. Article 18.</p>		
<p>Denmark, Act no. 602 of 12 June 2013 on the Danish Defence Intelligence Service (DDIS) (<i>Lov nr. 602 af 12. juni 2013 om</i></p>	<p>In accordance with Articles 4 – 6, <u>access/processing of personal data</u> is largely equivalent to the PET-</p>	<p>Not regulated in relation to Article 9. The safeguards in Articles 6, 10 and 15 apply <u>only</u> to:</p>	<p>The DDIS Act is <u>geographical neutral</u>, but please see the previous column.</p>

<p>Please, list law(s) providing for the protection of privacy and data protection against unlawful surveillance</p>	<p>List specific privacy and data protection safeguards put in place by this law(s)</p>	<p>Indicate whether rules on protection of privacy and data protection apply:</p> <p>only to nationals or also to EU citizens and/or third country nationals</p>	<p>Indicate whether rules on protection of privacy and data protection apply:</p> <p>only inside the country, or also outside (including differentiation if EU or outside EU)</p>
<p><i>Forsvarets Efterretningstjeneste (FE)).</i></p>	<p>Act, cf. the above, but apply <u>only</u> to:</p> <ol style="list-style-type: none"> 1) Danish citizens 2) Nordic citizens and foreigners with Danish legal residence permits, 3) Asylum seekers with known residence in Denmark of more than 6 months, and 4) Undertakings etc. domiciled in Denmark. <p><u>Rights to insight:</u> Individuals/undertakings can file a complaint to the Oversight Committee and – under extraordinary circumstances – gain partly or full insight in information about them, cf. Article 9. Individuals/undertakings can ask the Oversight Committee to make sure that DDIS is not illegally processing</p>	<ol style="list-style-type: none"> 1) Danish citizens 2) Nordic citizens and foreigners with Danish legal residence permits, and 3) Asylum seekers with known residence in Denmark of more than 6 months 4) Undertakings etc. domiciled in Denmark. 	

<p>Please, list law(s) providing for the protection of privacy and data protection against unlawful surveillance</p>	<p>List specific privacy and data protection safeguards put in place by this law(s)</p>	<p>Indicate whether rules on protection of privacy and data protection apply:</p> <p>only to nationals or also to EU citizens and/or third country nationals</p>	<p>Indicate whether rules on protection of privacy and data protection apply:</p> <p>only inside the country, or also outside (including differentiation if EU or outside EU)</p>
	<p>personal data about them, cf. Article 10. Individuals/undertakings can file a complaint to the Oversight to make sure that DDIS observes the rules on the processing of personal data set out in the DDIS act, cf. Article 15.</p>		
<p>Denmark, Act no. 378 of 6 July 1988 on the establishment of a committee on the DDIS and PET as amended by Act no. 632 of 12 June (Lov nr. 378 af 6. juli 1988 om etablering af et udvalg vedrørende Efterretningstjenesterne, som ændret ved lov nr. 632 af 12. juni 2013).</p>	<p>The Government has to provide the Committee with an annual briefing on the activities of PET and DDIS, including PET' use of agents and coercive measures not approved by the courts, cf. Article 2.</p>	<p>Not relevant.</p>	<p>Not relevant.</p>
<p>Denmark, Act no. 713 of 25 June 2014 on The Danish Centre for Cyber Security (CfCS) (Lov nr. 713 af 25. juni 2014 om</p>	<p><u>Right to deletion</u>: When the purpose of the processing is fulfilled. Anyhow, data related to a security threat shall be deleted</p>	<p>Not regulated.</p>	<p>Not regulated.</p>

<p>Please, list law(s) providing for the protection of privacy and data protection against unlawful surveillance</p>	<p>List specific privacy and data protection safeguards put in place by this law(s)</p>	<p>Indicate whether rules on protection of privacy and data protection apply:</p> <p>only to nationals or also to EU citizens and/or third country nationals</p>	<p>Indicate whether rules on protection of privacy and data protection apply:</p> <p>only inside the country, or also outside (including differentiation if EU or outside EU)</p>
<p><i>Center for Cybersikkerhed).</i></p>	<p>within 3 years, other data within 13 months, cf. Article 17.</p> <p><u>Right to challenge:</u> Individuals/undertakings can file a complaint to the Oversight Committee to make sure that the rules on the processing of personal data are observed, cf. Article 20.</p>		
<p>Denmark, Administrative Order no. 988 of 28 September 2006 on Data Retention as amended by Administrative Order no. 660 of 19 June 2014 (<i>Logningsbekendtgørelsen, bekendtgørelse nr. 988 af 28. september 2006, som ændret ved bekendtgørelse nr. 660 af 19. juni 2014</i>).</p>	<p><u>Right to deletion:</u> After 1 year, cf. Article 9.</p> <p>The pass on to and processing of data by the police shall be conducted in accordance with the rules on coercive and investigative measures in the Administration of Justice Act, cf. the above.</p>	<p>Not regulated.</p>	<p>Not regulated.</p>

1.5 Annex 2 – Oversight bodies and mechanisms

Name of the body/mechanism	Type of the body/mechanism	Legal basis	Type of oversight	Staff	Powers
<i>in English as well as in national language</i>	<i>e.g. parliamentary, executive/government, judicial, etc.</i>	<i>name of the relevant law, incl. specific provision</i>	<i>ex ante / ex post / both/ during the surveillance/etc. as well as whether such oversight is ongoing/regularly repeated</i>	<i>including the method of appointment of the head of such body AND indicate a total number of staff (total number of supporting staff as well as a total number of governing/managing staff) of such body</i>	<i>e.g. issuing legally binding or non-binding decisions, recommendations, reporting obligation to the parliament, etc.</i>
The national (district) courts (<i>Domstolene</i>)	Judicial	The Administration of Justice Act, book no. 4, second paragraph.	Ex ante and during surveillance.	Ordinary national courts.	Legally binding court orders.
The Oversight Committee of PET and DDIS (<i>Tilsynet med efterretningstjenestene</i>)	Executive.	The PET Act, Articles 16 – 22. The DDIS Act, Articles 13 – 19. The CfCS Act, Articles 19 – 24. The Act on the Parliamentary Control Committee, Article 1 – 3. For references, please see the above.	Ex post and potentially during the surveillance.	Composed of five members, appointed by for a four-year mandate. The chair, a judge of the High Court, is nominated by the presidents of the High Courts of Eastern and Western Denmark and appointed by the Minister of Justice. Other members are appointed by the Minister of Justice on the basis of discussions with the Parliamentary Control	Prescribes – in a legally binding manner – PET and DDIS to allow individuals/undertakings insight and delete information about them. Criticize, makes recommendations and expresses its opinion to PET. These are not legally binding, but it is implied that they are observed, cf. the wording and the preparatory works, and if not followed, PET shall

				<p>Committee, cf. Article 2a of the Act on the Parliamentary Control Committee.</p> <p>The Oversight Committee has its own secretariat.</p> <p>However, the number of supporting staff is not available.</p>	<p>inform the Oversight Committee and the matter must be submitted to the Minister of Justice to decision.</p> <p>PET is thus prescribed a duty to involve the Minister of Justice and due to that involvement the Minister of Justice thus holds the final responsibility.</p> <p>Furthermore, the Oversight Committee can inform the Minister of Justice about relevant and important issues.</p> <p>The Oversight Committee also holds the power to demand of PET all information necessary to conduct their activities and to demand access to premises from which PET conducts analyses etc.</p>
<p>The Parliamentary Control Committee (<i>Udvalget vedrørende Efterretningstjenesterne, Folketingets Kontroludvalg</i>)</p>	Parliamentary	<p>The Act on the parliamentary Control Committee, Article 1 – 3.</p>	Ex post.	<p>Composed of 5 members of Parliament appointed by the political parties seated in the presidium of the Danish Parliament.</p> <p>The chair is appointed by the Committee itself.</p> <p>According to Section 1(4) of the Act on the Parliamentary</p>	<p>The Government shall provide the Parliamentary Control Committee with an annual briefing on the activities of PET and DDIS. Furthermore, the Government shall keep the Control Committee informed about important</p>

				<p>Control Committee, the Control Committee is assigned a Secretary, who is not a member of Parliament, but a servant of the Parliament.</p> <p>According to the web page of the Parliament, the Control Committee is assigned two secretaries.</p>	<p>security- and foreign-policy related issues, and, on request by the Control Committee, also information, including statistics, about the activities of PET and DDIS. The Control Committee can also apply the Minister of Justice to demand the presence of the directors of PET and DDIS at the meetings of the Control Committee.</p> <p>Prior the issuance of new guidelines on the activities of PET and DDIS, the Control Committee must be informed of this by the Government.</p> <p>Prior to PET's annual report to the Parliament on the activities of PET, the annual report must be submitted to the Control Committee by the Government.</p> <p>Finally the Control Committee can make non-legally binding statements to the Government about issues discussed in the Committee and can make reports to the Parliament.</p>
--	--	--	--	---	--

					These reports are not annual, but could be. Since 1988 the Control Committee has submitted 8 reports on its activities. The reports are submitted with a view to publication. ³³
The Danish Data Protection Agency (<i>Datatilsynet</i>).	Executive.	The Act on Processing of Personal Data (<i>Persondataloven</i>), Articles 55 ff.	Ex post.	The Agency is composed of a Council and a Secretariat, presided by a director. The Council is appointed by the Minister of Justice and is composed of a chair, who is judge, and 6 members. As of 2013 the Secretariat engages 36 staff members.	The decisions of the Agency are legally binding, but do not apply to the activities of PET, DDIS and CfCS.

³³ Denmark, Bill no. 162 of 27 February 2013 on the Act amending the Act on the establishment of a Parliamentary Committee regarding DDIS and PET (*Lovforslag nr. 162 af 27. februar 2013 om lov om ændring af lov om etablering af et udvalg af Forsvarets og Politiets Efterretningstjenester*), available in Danish at: <https://www.retsinformation.dk/Forms/R0710.aspx?id=145508>.

1.6 Annex 3 – Remedies³⁴

The Danish Administration of Justice Act – coercive and investigative measures.				
Stages of surveillance process	Is the subject informed?	Does the subject have a right of access to the data collected on him/her?	List remedies available to an individual concerned	Legal basis for using the available remedies
	<i>Yes/No</i>	<i>Yes/No, please provide details if needed</i>	<i>Please list the type of remedial action that can be taken: e.g.: claims lodged with court(s), claims lodged with the oversight body, request to the surveillance authority, etc. AND please specify also the name (e.g. Supreme Court) and type of the body (e.g. judicial, executive, parliamentary) providing such remedies.</i>	<i>Violation of data protection, private life, specific legislation, etc.</i>
Collection*	No	Not regulated.	Prior court order.	Please see the previous column.
Analysis*	n/a	n/a	n/a	n/a
Storing*	n/a	n/a	n/a	n/a
Destruction*	n/a	n/a	n/a	n/a
After the whole surveillance process has ended	Yes, as a main rule.	Not regulated.	n/a	n/a

³⁴ In case of different remedial procedures please replicate the table for each legal regime.

* For the definitions of these terms, please refer to the FRA/CoE (2014), *Handbook on European data protection law*, Luxembourg, 2014, pp. 46-47, available at: <http://fra.europa.eu/en/news/2014/council-europe-and-eu-fundamental-rights-agency-launch-handbook-european-data-protection>

The PET Act				
Stages of surveillance process	Is the subject informed?	Does the subject have a right of access to the data collected on him/her?	List remedies available to an individual concerned	Legal basis for using the available remedies
Collection*	No	No/Yes, cf. next column.	The subject can file complaints to the Oversight Committee (executive) in order to 1) In extraordinary cases, to gain partly/full insight in information being processed about them by PET, cf. Article 12, 2) to make sure, that PET is not illegally processing information about them, cf. Article 13, and 3) to make sure that PET oversees the rules on the processing of personal data, cf. Article 18.	Violation of the PET Act – access to collect information. Violation of data protection rules as set out in the PET Act.
Analysis*	No	No/Yes, cf. next column.	Please see the above.	Please see the above.
Storing*	No	No/Yes, cf. next column.	Please see the above.	Please see the above.
Destruction*	No	No/Yes, cf. next column.	Please see the above.	Please see the above.

* For the definitions of these terms, please refer to the FRA/CoE (2014), *Handbook on European data protection law*, Luxembourg, 2014, pp. 46-47, available at: <http://fra.europa.eu/en/news/2014/council-europe-and-eu-fundamental-rights-agency-launch-handbook-european-data-protection>

After the whole surveillance process has ended	No/Yes (as a main rule) in relation to coercive and investigative measures conducted in accordance with the Administration of Justice Act, cf. the above.	No/Yes, cf. next column.	Please see the above.	Please see the above.
---	---	--------------------------	-----------------------	-----------------------

The DDIS Act				
Stages of surveillance process	Is the subject informed?	Does the subject have a right of access to the data collected on him/her?	List remedies available to an individual concerned	Legal basis for using the available remedies
Collection*	No	No/Yes, cf. next column.	<p>The subject can file a complaint to the Oversight Committee (executive) in order to</p> <ol style="list-style-type: none"> 1) In extraordinary cases, to gain partly/full insight in information being processed about them by DDIS, cf. Article 9. <p>The subject - if Danish/Nordic citizen etc., please see the above, can file complaints to the Oversight Committee in order to</p> <ol style="list-style-type: none"> 1) make sure, that DDIS is not illegally processing information about them, cf. Article 10, 2) to make sure that PET oversees the rules on the processing of personal data, cf. Article 15. 	<p>Violation of the DDIS Act – acces to collect information.</p> <p>Violation of data protection rules as set out in the PET Act.</p>
Analysis*	No	No/Yes, cf. next column.	Please see the above.	Please see the above.
Storing*	No	No/Yes, cf. next column.	Please see the above.	Please see the above.

* For the definitions of these terms, please refer to the FRA/CoE (2014), *Handbook on European data protection law*, Luxembourg, 2014, pp. 46-47, available at: <http://fra.europa.eu/en/news/2014/council-europe-and-eu-fundamental-rights-agency-launch-handbook-european-data-protection>

Destruction *	No	No/Yes, cf. next column.	Please see the above.	Please see the above.
After the whole surveillance process has ended	No.	No/Yes, cf. next column.	Please see the above.	Please see the above.

The Act on the Danish Centre for Cyber Security (CfCS)				
Stages of surveillance process	Is the subject informed?	Does the subject have a right of access to the data collected on him/her?	List remedies available to an individual concerned	Legal basis for using the available remedies
Collection *	No.	Not regulated.	Complaint can be filed to the Oversight Committee, cf. Article 20. In the preparatory works to the CfCS Act reference is made to the practice of the Oversight Committee in relation to the oversight of the activities of PET and DDIS. From the preparatory works of the PET Act it follows that anyone protected by the safeguards in the PET Act can file a complaint to the Oversight Committee. The Committee is, however, entitled to decide whether a complaint in fact requires an investigation and the Committee thus has the power to reject a complaint.	Violation of data protection as regulated in the CfCS Act.
Analysis *	No	Not regulated.	Please see the above.	Please see the above.
Storing *	No	Not regulated.	Please see the above.	Please see the above.
Destruction *	No	Not regulated.	Please see the above.	Please see the above.
After the whole surveillance process has ended	No	Not regulated.	Please see the above.	Please see the above.

23

* For the definitions of these terms, please refer to the FRA/CoE (2014), *Handbook on European data protection law*, Luxembourg, 2014, pp. 46-47, available at: <http://fra.europa.eu/en/news/2014/council-europe-and-eu-fundamental-rights-agency-launch-handbook-european-data-protection>

Administrative Order on Data retention				
Stages of surveillance process	Is the subject informed?	Does the subject have a right of access to the data collected on him/her?	List remedies available to an individual concerned	Legal basis for using the available remedies
Collection *	No	Not regulated.	No remedies available.	Please see the previous column.
Analysis *	No	Not regulated.	No remedies available.	Please see the previous column.
Storing *	No	Not regulated.	No remedies available.	Please see the previous column.
Destruction *	No	Not regulated.	No remedies available.	Please see the previous column.
After the whole surveillance process has ended	No, only (as a main rule) if data is passed on to the police in accordance with the rules on coercive measures and investigative measures conducted in accordance with the Administration of Justice Act, cf. the above.	Not regulated.	No remedies available. (However, the passing on of data to the police requires a prior court order. This is the safeguard mechanism.)	Please see the previous column.

* For the definitions of these terms, please refer to the FRA/CoE (2014), *Handbook on European data protection law*, Luxembourg, 2014, pp. 46-47, available at: <http://fra.europa.eu/en/news/2014/council-europe-and-eu-fundamental-rights-agency-launch-handbook-european-data-protection>

1.7 Annex 4 – Surveillance-related case law at national level

Please provide a maximum of three of the most important national cases relating to surveillance. Use the table template below and put each case in a separate table.

The related case law primarily concern details of the use of coercive measures in accordance with Administration of Justice Act. This is not entirely relevant in relation to this report. However, some examples will follow below.

No law suit was initiated based on the Snowden revelations. However, it could be of the interest that Snowden recently commented on a current Danish case on the media scandal following the revelations by a former reporter from the magazine *Se og Hør* according to which the magazine for a number of years has conducted surveillance of celebrities and the royal family based on information on their credit card transactions from a leak within the Nordic provider of payment, credit card and information systems (NETS). Further information is available at: <http://politiken.dk/indland/politik/ECE2279894/snowden-blander-sig-i-se-og-hoer-skandale-og-dansk-debat-om-overvaagning/>.

Case title	
Decision date	6 December 2006
Reference details (type and title of court/body; in original language and English [official translation, if available])	U 2007.727 Ø (Decision of High Court of Eastern Denmark)
Key facts of the case (max. 500 chars)	<p>A person was charged with terrorism.</p> <p>The defendant applied for access to court orders used for a telephone tapping conducted by PET in <u>another</u> case.</p> <p>Access was permitted as the court orders were assumed to be of importance to the case concerned.</p>

Main reasoning/argumentation (max. 500 chars)	The defendant has the right to access to all documents/information of importance to the case, cf. the preparatory works of the Administration of Justice Act and ECHR Article 6, no matter if the information is obtained in relation to the case in question
Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	Please see the above.
Results (sanctions) and key consequences or implications of the case (max. 500 chars)	Access was accepted.

Case title	
Decision date	17 February 2006
Reference details (type and title of court/body; in original language and English [official translation, if available])	U 2006.1596 Ø (Decision of the High Court of Eastern Denmark)

<p>Key facts of the case (max. 500 chars)</p>	<p>Four people had been charged with terrorism on the basis of telephone tapping conducted by PET.</p> <p>The defendants applied for access to the court orders that allowed the phone tapping with reference to the preparatory works of the Administration of Justice Act and ECHR Article 6 according to which a defendant has the right to all documents/information of importance to the case.</p> <p>However, the defendants were denied access as the facts they were looking to find in the court orders were assumed to have no importance to case.</p>
<p>Main reasoning/argumentation (max. 500 chars)</p>	<p>The defendant has the right to access to all documents/information of importance to the case. However, if the information has no importance to the case, access is denied.</p>
<p>Key issues (concepts, interpretations) clarified by the case (max. 500 chars)</p>	<p>In relation to the secrecy of the intelligence services, during trial, under certain circumstances the defendant can gain access to/insight in court orders allowing surveillance.</p>
<p>Results (sanctions) and key consequences or implications of the case (max. 500 chars)</p>	<p>Access was denied in the specific case.</p>

Case title	
Decision date	19 March 2001
Reference details (type and title of court/body; in original language and English [official translation, if available])	U 2001.1276 H (Decision of the Supreme Court)
Key facts of the case (max. 500 chars)	<p>In relation to the investigation of a narcotics case, the police requested a court order under Section 791 a of the Administration of Justice Act on “observation” in order to install “sniffer software” in the computer of a suspect. The software would allow the police to gain insight in what would be written on the computer.</p> <p>The district court denied to issue a court order.</p> <p>The decision was then reversed by the the High Court of Eastern Denmark.</p> <p>Finally, the Supreme Court considered the installation of the software equivalent to a repeated secret “search of premises” and <u>not</u> “observation”, cf. Section 791 a of the Administration of Justice Act. A court order was thus denied.</p>
Main reasoning/argumentation (max. 500 chars)	The installation of “sniffer software” in the computer of a suspect is not equivalent to an “observation”, but a repeated secret “search of premises”.

Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	The case reflects the considerations of the courts when issuing a court order.
Results (sanctions) and key consequences or implications of the case (max. 500 chars)	Court order was denied.

1.8 Annex 5 – Key stakeholders at national level

Please list all the key stakeholders in your country working in the area of surveillance and divide them according to their type (i.e. public authorities, civil society organisations, academia, government, courts, parliament, other). Please provide name, website and contact details.

Name of stakeholder (in English as well as your national language)	Type of stakeholder <i>(i.e. public authorities, civil society organisations, academia, government, courts, parliament, other)</i>	Contact details	Website
The Danish Ministry of Justice <i>(Justitsministeriet)</i>	Public authority	Justitsministeriet Slotsholmsgade 10 1216 København K Denmark Phone: +45 72 26 84 00 Fax: +45 33 93 35 10 E-mail: jm@jm.dk	www.jm.dk
The Danish Ministry of Defence <i>(Forsvarsministeriet)</i>	Public authority	Forsvarsministeriet Holmens Kanal 42 1060 København K Denmark Phone: +45 33 92 33 20	www.fmn.dk

		Fax: +45 33 32 06 55 E-mail: fmn@fmn.dk	
The Danish National Police <i>(Rigspolitiet)</i>	Public authority	Rigspolitiet Polititorvet 14 1780 København V Denmark Phone: + 45 33 14 88 88 E-mail: politi@politi.dk	www.politi.dk
The Danish Security and Intelligence Service <i>(Politiets Efterretningstjeneste (PET))</i>	Public authority	Politiets Efterretningstjeneste Klausdalsbrovej 1 2860 Søborg Denmark Phone: +45 45 15 90 07 Fax: +45 45 15 01 90 E-mail: pet@pet.dk	www.pet.dk
The Danish Defence Intelligence Service (DDIS) <i>(Forsvarets Efterretningstjeneste (FE))</i>	Public authority	Forsvarets Efterretningstjeneste Kastellet 30 2100 København Ø Denmark Phone: + 45 33 32 55 66 Fax: +45 33 93 13 20 E-mail: fe@fe-mail.dk	www.fe-ddis.dk

<p>The Danish Centre for Cyber Security (<i>Center for Cybersikkerhed</i>)</p>	<p>Public authority (part of DDIS)</p>	<p>Center for Cybersikkerhed Kastellet 30 (postal adress) Østbanegade 83 (adress for visits) 2100 København Ø Denmark Phone: +45 3332 5580 E-mail: cfcs@cfcs.dk</p>	<p>http://fe-ddis.dk/cfcs/Pages/cfcs.aspx</p>
<p>The Oversight Committee of PET and DDIS (<i>Tilsynet med Efterretningstjenesterne</i>)</p>	<p>Excutive authority.</p>	<p>Tilsynet med Efterretningstjenesterne Borgergade 28, 1. sal 1300 København K Denmark Phone: +45 25 50 10 34</p>	<p>www.tilmet.dk</p>
<p>The Parliamentary Control Committee (<i>Folketingets Udvalg vedrørende efterretningstjenesterne, "Kontroludvalget"</i>)</p>	<p>Parliamentary Committee</p>	<p>Folketinget Christiansborg 1240 København K Denmark Phone: +45 3337 5500 E-mail: folketinget@ft.dk</p>	<p>http://www.ft.dk/Folketinget/udvalg_delegationer_kommissioner/Udvalg/Udvalget_vedr_efterretningstjenesterne.aspx</p>
<p>Danish Data Protection Agency (<i>Datatilsynet</i>)</p>	<p>Public authority</p>	<p>Datatilsynet Borgergade 28,5 1300 København K Denmark</p>	<p>www.datatilsynet.dk</p>

		Phone: +45 33 19 32 00 Fax: +45 33 19 32 18 E-mail: dt@datatilsynet.dk	
The Courts of Denmark <i>(Domstolene)</i>	Courts	Domstolsstyrelsen <i>(The Danish Court Administration)</i> Store Kongensgade 1-3 1264 København K Denmark E-mail: post@domstolsstyrelsen.dk	www.domstol.dk
The Council for Digital Security <i>(Rådet for Digital Sikkerhed)</i>	Independent Member organization (NGO)	Rådet for Digital Sikkerhed Toldbodgade 12 1253 Copenhagen K Denmark e-mail: info@digitalsikkerhed.dk	www.digitalsikkerhed.dk
CEPOS	Independent liberal think tank.	CEPOS Landgreven 3, 3. sal 1301 København K Phone: + 45 33 45 60 30 Fax: +45 33 45 60 45 E-mail: info@cepos.dk	www.cepos.dk
The Danish Institute for Human Rights <i>(Institut for Menneskerettigheder)</i>	National Human Rights Institution	Institut for Menneskerettigheder Wilders Plads 8K 1403 København K	www.humanrights.dk

		Denmark Phone: +45 32 69 88 88 Fax: +45 32 69 88 00 E-mail: info@humanrights.dk	
--	--	---	--

1.9 Annex 6 – Indicative bibliography

Please list relevant reports, articles, studies, speeches and statements divided by the following type of **sources** (*in accordance with FRA style guide*):

1. Government/ministries/public authorities in charge of surveillance

National legislation (chronological order, newest first)

Denmark, The Danish Penal Code, Consolidated act no. 871 of 4 July 2014 (*Straffeloven, lovbekendtgørelse nr. 871 af 4. juli 2014*), available in Danish at: <https://www.retsinformation.dk/Forms/R0710.aspx?id=164192>.

Denmark, Act no. 713 of 25 June 2014 on The Danish Centre for Cyber Security (*Lov nr. 713 af 25. juni 2014 om Center for Cybersikkerhed*), available in Danish at: <https://www.retsinformation.dk/Forms/R0710.aspx?id=163853>.

Denmark, Administrative Order no. 988 of 28 September 2006 on Data Retention as amended by Administrative Order no. 660 of 19 June 2014 (*Logningsbekendtgørelsen, Bekendtgørelse nr. 988 af 28. september 2006 som ændret ved bekendtgørelse nr. 660 af 19 June 2014*), available in Danish at: <https://www.retsinformation.dk/Forms/R0710.aspx?id=2445>.

Denmark, The Danish Public Administration Act, Consolidated Act no. 433 of 22 April 2014 (*Forvaltningsloven, lovbekendtgørelse nr. 433 af 22. april 2014*), available in Danish at: <https://www.retsinformation.dk/Forms/R0710.aspx?id=161411>.

Denmark, Act no. 604 of 12 June 2013 on the Danish Security and Intelligence Service as amended by Act. no. 1624 of 26 December 2013 (*Lov nr. 604 af 12. juni 2013 om Politiets Efterretningstjeneste (PET,) som ændret ved lov nr. 1624 af 26. december 2013*), available in Danish at: <https://www.retsinformation.dk/Forms/R0710.aspx?id=152182>.

Denmark, The Danish Administration of Justice Act, Consolidated act no. 1139 of 24 September 2013, (*Retsplejeloven, lovbekendtgørelse nr. 1139 af 24. september 2013*), available in Danish at: <https://www.retsinformation.dk/Forms/R0710.aspx?id=157953>.

Denmark, Act no. 632 of 12 June 2013 amending the Act on establishing a committee on the Danish Defence Intelligence Service and the Danish Security and Intelligence Service (*Lov nr. 632 af 12. juni 2013 om ændring af lov om etablering af et udvalg om forsvarrets og politiets efterretningstjenester*), available in Danish at: www.retsinformation.dk/Forms/r0710.aspx?id=152183.

Denmark, Act no. 378 of 6 July 1988 on the establishment of a committee on the Danish Defence intelligence Agency and the Danish Security and Intelligence Service as amended by Act no. 632 of 12 June 2013 (*Lov nr. 378 af 6. juli 1988 som ændret ved lov nr. 632 af 12. juni 2013*), available in Danish at: <https://www.retsinformation.dk/Forms/R0710.aspx?id=59424>.

Denmark, The Danish Public Information Act, Act no. 606 of 12 June 2013 (*Offentlighedsloven, lov nr. 606 af 12. juni 2013*), available in Danish at: <https://www.retsinformation.dk/Forms/R0710.aspx?id=152299>.

Denmark, Act no. 602 of 12 June 2013 on the Danish Defence Intelligence Service (*Lov nr. 602 af 12. juni 2013 om Forsvarets Efterretningstjeneste (FE)*), available in Danish at: www.retsinformation.dk/Forms/r0710.aspx?id=152195.

Denmark, Act no. 429 of 31 May 2000 on Processing of Personal Data with later amendments (*Persondataloven, Lov nr. 429 af 31. maj 2000 om behandling af personoplysninger med senere ændringer*), available in Danish at: www.retsinformation.dk/Forms/R0710.aspx?id=828.

Denmark, The Danish Constitution, Act. No. 169 of 5 June 1953 (*Grundloven, Lov nr. 169 af 5. juni 1953*), available in Danish at: <https://www.retsinformation.dk/Forms/R0710.aspx?id=45902>, available in English at: <http://www.eu-oplysningen.dk/upload/application/pdf/0172b719/Constitution%20of%20Denmark.pdf>.

National legislation, Preparatory works (chronological order, newest first)

Denmark, Bill no. 192 of 8 May 2014 on the Act on the Danish Centre for Cyber Security (*Lovforslag nr. 192 af 8. Maj 2014 om Center for Cybersikkerhed*), available in Danish at: <https://www.retsinformation.dk/Forms/R0710.aspx?id=162037>.

Denmark, Bill no. 163 of 27 February 2013 on the Danish Defence Intelligence Service, (*Lovforslag nr. 163 af 27. februar 2013 om Forsvarets Efterretningstjeneste (FE)*), available in Danish at: <https://www.retsinformation.dk/Forms/R0710.aspx?id=145518>

Denmark, Bill no. 162 of 27 February 2013, amending the Act no. 378 of 6 July 1988 on the establishment of a committee on the Danish Defence intelligence Agency and the Danish Security and Intelligence Service (*Lovforslag nr. 162 af 27. februar 2013 om ændring af lov nr. 378 af 6. juli 1988 om etablering af et udvalg om forsvarets og politiets efterretningstjenester*), available in Danish at: <https://www.retsinformation.dk/Forms/R0710.aspx?id=145508>.

Denmark, Report no. 1529/2012 of the Expert Committee on the Danish Security and Intelligence Service and the Danish Defence Intelligence Service (*Betænkning nr. 1529/2012 om PET og FE*), February 2012, available in Danish at http://www.statensnet.dk/betaenkninger/1401-1600/1529-2012/1529-2012_pdf/printversion_1529-2012.pdf.

Denmark, Ministry of Justice (*Justitsministeriet*), "*Oversigt over Høringssvar*", 14 December 2011, available in Danish at: http://webarkiv.ft.dk/img20012/udvtilag/lib9/20012_1119.pdf.

Case-law (chronological, newest first)

Court of Justice of the European Union in joined cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger and Others*, available in English at: <http://curia.europa.eu/juris/document/document.jsf?jsessionid=9ea7d2dc30d56133de37ca3a4ac788e6c47800df875e.e34KaxiLc3qMb40Rch0SaxuNc3v0?text=&docid=150642&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=357930>.

The Danish Supreme Court, Decision of 19 March 2001, UfR 2001.1276 H (Access requires subscription to UfR).

The High Court of Easter Denmark, Decision of 17 February 2006, UfR 2006.1596 Ø (Access requires subscription to UfR).

The High Court of Eastern Denmark, Decision of 6 December 2006, UfR 2007.727 Ø (Access requires subscription to UfR).

Reports, Statements etc.

Denmark, Ministry of Justice (*Justitsministeriet*) (2014), "Justitsministeren ophæver reglerne om sessionslogging", Press release, 2 June 2014, information available in Danish at: <http://www.justitsministeriet.dk/nyt-og-presse/pressemeddelelser/2014/justitsministeren-oph%C3%A6ver-reglerne-om-sessionslogging>.

Denmark, Ministry of Justice (*Justitsministeriet*) (2014), "*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*", 2 June 2014, available in Danish at: <http://justitsministeriet.dk/sites/default/files/media/Pressemeddelelser/pdf/2014/Notat%20om%20logningsdirektivet.pdf>.

Denmark, Data Protection Agency (*Datatilsynet*) (2013), Annual report 2012, available in Danish at: http://www.datatilsynet.dk/fileadmin/user_upload/dokumenter/AArsberetninger/Aarsberet_2012.pdf.

Hyperlinks (alphabetical order)

CEPOS (*CEPOS*), information available at: www.cepos.dk.

The Council for Digital Security (*Rådet for Digital Sikkerhed*), information available at: www.digitalsikkerhed.dk.

The Danish Centre for Cyber Security (*Center for Cybersikkerhed*), information available at: <http://fe-ddis.dk/cfcs/Pages/cfcs.aspx>.

The Danish National Courts (*Domstolene*), information available at: www.domstol.dk.

The Danish Data Protection Agency (*Datatilsynet*), information available at: www.datatilsynet.dk.

The Danish Defence Intelligence Service (*Forsvarets Efterretningstjeneste*), information available at: www.fe-ddis.dk.

The Danish Institute for Human Rights (*Institut for Menneskerettigheder*), information available at: www.humanrights.dk.

The Danish Ministry of Defence (*Forsvarsministeriet (FE)*), information available at: www.fmn.dk.

The Danish Ministry of Justice (*Justitsministeriet*), information available at: www.jm.dk.

The Danish National Police (*Rigspolitiet*), information available at: www.politi.dk.

The Danish Security and Intelligence Service (*Politiets Efterretningstjeneste (PET)*), information available at: <https://www.pet.dk/English/About%20PET.aspx>.

The Oversight Committee of PET and DDIS (*Tilsynet med Efterretningstjenesterne*), information available at: www.tilmet.dk.

The Parliamentary Control Committee (*Folketingets udvalg vedrørende Efterretningstjenesterne, "Kontroludvalget"*), information available at: http://www.ft.dk/Folketinget/udvalg_delegationer_kommissioner/Udvalg/Udvalget_vedr_efterretningstjenesterne.aspx.

2. National human rights institutions, ombudsperson institutions, national data protection authorities and other national non-judicial bodies/authorities monitoring or supervising implementation of human rights with a particular interest in surveillance.

Legal briefs (chronological, newest first)

Danish Institute for Human Rights (*Institut for Menneskerettigheder*), (2014), "*Med udkastet til en ny lov om Center for Cybersikkerhed øger regeringen myndighedernes mulighed for at overvåge danske borgere og virksomheder. Samtidig får offentligheden sværere ved at føre kontrol med overvågningen*", 5 March 2014, information available in Danish at: <http://menneskeret.dk/nyheder/ny-lov-datasikkerhed-moeder-kritik>.

Danish Institute for Human Rights (*Institut for Menneskerettigheder*), (2014), "*Høring over udkast til lov om Center for Cybersikkerhed samt evaluering af GovCERT-loven*", j.no. 540.10/30403/RFJ7MAF, 4 March 2014, available in Danish at: http://menneskeret.dk/files/media/hoeringssvar/hoeringssvar_afgivet_i_2014/marts%202014/marts_2014_tilgaengeligt/24_b_center_for_cybersikkerhed.pdf.

Danish Institute for Human Rights (*Institut for Menneskerettigheder*), (2013), "*Høring over udkast til forslag til lov om ændring af lov om etablering af et udvalg om forsvarets og politiets efterretningstjenester (styrkelse af den parlamentariske kontrol og indsigt)*", j. no.540.10/28538/HSC/JCH, 11 February 2013, available in Danish at: http://menneskeret.dk/files/media/hoeringssvar/h%C3%B8ringssvar_afgivet_i_2013/februar_2013/24_b_styrkelse_af_kontroludvalget.pdf.

Danish Institute for Human Rights (*Institut for Menneskerettigheder*) (2012), '*Høring over betænkning nr. 1592/2012 om PET og FE*', j. no. 540.10/27157/PVK/ SWG/RFJ/HSC, 8 June 2012, available in Danish at: http://menneskeret.dk/files/media/hoeringssvar/hoeringssvar_afgivet_i_2012/juni_2012/50_b_betaenkning_om_pet_og_fe.pdf.

Reports

Danish Institute for Human Rights (*Institut for Menneskerettigheder*), (2013), “*Status 2013: Databeskyttelse*”, available in Danish at: http://menneskeret.dk/files/media/dokumenter/status/2013/status_2013_imr_databeskyttelse.pdf. Summary available in English at: <http://www.humanrights.dk/publications/status-2013>.

Other (chronological, newest first)

Berlingske (2014), ”Bred enighed: Ny terrorkommission skal være bredt sammensat”, 12 August 2014, available in Danish at: <http://www.b.dk/politiko/bred-enighed-ny-terrorkommission-skal-vaere-bredt-sammensat>.

Berlingske (2014), “Vestre: Du skal have besked, når det offentlige lurere på dig”, 30 July 2014, available in Danish at: <http://www.b.dk/politiko/venstre-du-skal-have-besked-naar-det-offentlige-lurer-paa-dig>.

Berlingske (2014), “SF vil styrke tilsynet med PET og FE”, 21 July 2014, available in Danish at: <http://www.b.dk/politiko/sf-vil-styrke-tilsynet-med-pet-og-fe>.

Berlingske, (2012), “PET-lov risikerer at blive en papirtiger”, 22 September 2012, feature by Jonas Christoffersen, director, and Louise Holck, deputy director, Danish Institute for Human Rights (*Institut for Menneskerettigheder*), available in Danish at: <http://www.b.dk/kronikker/pet-lov-risikerer-at-blive-en-papirtiger#comments-wrapper>.

3. Non-governmental organisations (NGOs)

The Council for Digital Security (*Rådet for Digital Sikkerhed*), (2014), ”*Høring over udkast til lov om Center for Cybersikkerhed*”, 4 March 2014, available in Danish at: http://www.digitalsikkerhed.dk/fileadmin/user_upload/20140304_RfDS_hoeringssvar_CFCS.pdf.

The Council for Digital Security (*Rådet for Digital Sikkerhed*), (2014), “*Information og anbefalinger nr. 1, Efterretningstjenesternes indsamling af data om borgerne*”, 5 February 2014, available in Danish at: http://www.digitalsikkerhed.dk/fileadmin/user_upload/20140205_RfDS_Info_anbefal_1_Efterretningstjenesters_indsamling.pdf.

4. Academic and research institutes, think tanks, investigative media report.

CEPOS

CEPOS, (2009), “*Den juridiske og parlamentariske kontrol med PET og FE er for svag*”, 21 June 2009, available in Danish at: http://cepos.dk/sites/default/files/analyse_publication/Den_juridiske_og_parlamentariske_kontrol_med_PET_og_FE_er_for_svag_og_boer_styrles.pdf.

Privacy International, the Electronic Privacy Information Center (EPIC) and the Center for Media and Communications Studies (CMCS)

Privacy International, the Electronic Privacy Information Center (EPIC) and the Center for Media and Communications Studies (CMCS), (2010), *European Privacy and Human Rights*, available in English at: <https://www.privacyinternational.org/sites/privacyinternational.org/files/file-downloads/ephr.pdf>.

University of Copenhagen

Artur Appazov, (2014), *Legal Aspects of Cybersecurity*, University of Copenhagen, Faculty of Law, available in English at: http://justitsministeriet.dk/sites/default/files/media/Arbejdsomraader/Forskning/Forskningspuljen/Legal_Aspects_of_Cybersecurity.pdf.