Short Thematic Report

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

Legal update

Country: United Kingdom

Version of 1 July 2016

FRANET contractor: Human Rights Law Centre, University of Nottingham

Author(s) name(s): Carly Nyst and An Cuypers
Reviewed by: Professor David Harris

1 Description of tasks – Phase 3 legal update

1.1 Summary

*FRANET contractors are requested to highlight in 1 to 2 pages **maximum** the key developments in the area of surveillance by intelligence services in their Member State. This introductory summary should enable the reader to have a snap shot of the evolution during the report period (last trimester of 2014 until mid-2016). It should in particular mention:*

1. *the legislative reform(s) that took place or are taking place and highlight the key aspect(s) of the reform.*
2. *the important (higher) court decisions in the area of surveillance*
3. *the reports and inquiry by oversight bodies (parliamentary committees, specialised expert bodies and data protection authorities) in relation to the Snowden revelations*
4. *the work of specific ad hoc parliamentary or non-parliamentary commission (for example the NSA inquiry of the German Parliament) discussing the Snowden revelations and/or the reform of the surveillance focusing on surveillance by intelligence services should be referred to.*

There have been substantial developments in both statutory and case law pertaining to surveillance by intelligence services in the United Kingdom since the previous report was submitted in September 2014. These developments, which include most notably the introduction of legislation overhauling the legal regime for interception and communications surveillance, but also extend to the publication of one parliamentary and two independent reviews of surveillance by intelligence services, and a number of higher court decisions, are outlined below in chronological order, in order to highlight the impact court decisions and independent reviews have had on the legislative reform process.

***Liberty & Others v. the Security Services*, judgements of 5 December 2014 and 6 February 2015**

In judgements delivered on 5 December 2014 and 6 February 2015, the Investigatory Powers Tribunal (IPT) made its first ever finding against the British security and intelligence services.[1] The Tribunal found that the claimants had successfully established that the legal regime by which British intelligence services received access to foreign intelligence material, and which underpinned UK access to the United States' PRISM and Upstream surveillance programmes, was insufficiently accessible to the public, albeit only prior to disclosures made during the course of the case. The Tribunal concluded in its 5 December 2014 judgement that because the government had publicly disclosed some of the substance of "below the waterline" policies pertaining to access to foreign intelligence material in response to the case brought by ten NGOs, including Liberty, Privacy International, and Amnesty International, the intelligence sharing regime was thenceforth sufficiently accessible so as to be compliant with Articles 8 and 10 of the European Convention on Human Rights (ECHR).[2]

With respect to the claimants' other claim, namely that the bulk interception of internet communications by the British intelligence services violated Articles 8 and 10 of the ECHR, the Tribunal held that the legal regime pertaining to bulk interception, namely that enshrined

[1] United Kingdom, Investigatory Powers Tribunal, *Liberty & Others v. the Security Service, SIS, GCHQ*, IPT/13/77/H, 5 December 2014, available at www.ipt-uk.com/docs/IPT_13_168-173_H.pdf; UK, Investigatory Powers Tribunal, *Liberty & Others v. the Security Service, SIS, GCHQ*, IPT/13/77/H, 6 February 2015, available at www.ipt-uk.com/docs/Liberty_Ors_Judgment_6Feb15.pdf.

[2] United Kingdom, Investigatory Powers Tribunal, *Liberty & Others v. the Security Service, SIS, GCHQ*, IPT/13/77/H, 5 December 2014, available at www.ipt-uk.com/docs/IPT_13_168-173_H.pdf.

in Section 8 (4) of the 2000 Regulation of Investigatory Powers Act (RIPA),[3] entailed no contravention of Articles 8 or 10. That is despite the fact the regime permitting interception is "not so targeted and not so limited, but [which] can extend to substantial quantities of communications […] contained in 'bearers' carrying communications to many countries".[4]

***Privacy and Security: A modern and transparent legal framework*, Report of the UK Parliament's Intelligence and Security Committee, 12 March 2015**

The Intelligence and Security Committee's (ISC)[5] review of surveillance by intelligence services was prompted by the revelations contained in the Snowden documents of the mass surveillance practices of Britain's signals intelligence agency, the UK Government Communications Headquarters (GCHQ).[6] The Committee's highly-redacted report constituted the first official recognition of the veracity of some of the claims in the Snowden documents, including the deployment of "bulk interception" by the UK intelligence services. It also revealed the existence of previously unknown capabilities to obtain "bulk personal datasets".[7]

Although the ISC accepted the need for reform of the legal framework underpinning surveillance by intelligence agencies – the current framework being "unnecessarily complicated and […] lack[ing] transparency",[8] it did not find any wrongdoing on the part of Britain's intelligence services, and rejected claims that British intelligence agencies have "the legal authority, the resources, the technical capability, or the desire to intercept every communication of British citizens, or of the internet as a whole".[9] Critically, the ISC report recommended the replacement of the current legal framework governing surveillance with a new Act of Parliament.[10]

***A Question of Trust*, Report of the Independent Reviewer of Terrorism Legislation, David Anderson, 11 June 2015**

In what has subsequently come to be regarded as the most comprehensive and authoritative review of surveillance by intelligence services in Britain, in June 2015 the Independent Reviewer of Terrorism Legislation, David Anderson, released a 300-page report of a lengthy investigation into the capabilities and practices of Britain's police and intelligence agencies, with extensive recommendations which have come to guide legislative reform in this area.[11] Mr Anderson joined the ISC in calling for wholesale reform of the legal framework, calling

---

[3] United Kingdom, HM Government (2000), *Regulation of Investigatory Powers Act 2000*, 28 July 2000, available at www.legislation.gov.uk/ukpga/2000/23.

[4] United Kingdom, Investigatory Powers Tribunal, *Liberty & Others v. the Security Service, SIS, GCHQ*, IPT/13/77/H, 5 December 2014, par. 93, available at www.ipt-uk.com/docs/IPT_13_168-173_H.pdf.

[5] For more information, see: United Kingdom, Intelligence and Security Committee of Parliament (ISC), http://isc.independent.gov.uk/.

[6] For more information, see: United Kingdom, UK Government Communications Headquarters, www.gchq.gov.uk.

[7] United Kingdom, Intelligence and Security Committee of Parliament (2015), *Privacy and Security: A modern and transparent legal framework*, 12 March 2015, available at http://tinyurl.com/zg95dez.

[8] United Kingdom, Intelligence and Security Committee of Parliament (2015), *Privacy and Security: A modern and transparent legal framework*, 12 March 2015, pp. 2, 7 and 11, available at http://tinyurl.com/zg95dez.

[9] United Kingdom, Intelligence and Security Committee of Parliament (2015), *Privacy and Security: A modern and transparent legal framework*, 12 March 2015, p. 2, available at http://tinyurl.com/zg95dez.

[10] United Kingdom, Intelligence and Security Committee of Parliament (2015), *Privacy and Security: A modern and transparent legal framework*, 12 March 2015, pp. 2 and 103, available at http://tinyurl.com/zg95dez.

[11] Anderson, D. (2015), *A question of trust: Report of the Investigatory Powers Review*, June 2015, available at http://tinyurl.com/obodyky.

the framework applicable to date "incomprehensible to all but a tiny band of initiates".[12] The report called for the eradication of the distinction between internal and external communications, the revision of the definitions of communications content and data, and the introduction of impartial judicial arbiters into the authorisation process pertaining to interception for communications. The report also endorsed the utility of bulk interception capabilities to the intelligence services, while reserving judgment on their conformity with the proportionality requirements of Article 8 of the ECHR.[13]

Liberty & Others v. the Security Services, judgement of 22 June 2015

Following on from its previous judgements concerning the legal regime concerning bulk interception and acquisition of foreign intelligence material, the Investigatory Powers Tribunal then turned to the factual examination of whether the claimants had in actual fact been subject to unlawful interception or had their communications acquired through the NSA prior to December 2014. In a judgment of 22 June 2015, it made determinations in favour of Amnesty International and the Legal Resources Centre, providing some factual basis for the findings in each.[14] The Tribunal refrained from making an explicit finding on the systemic proportionality of the Section 8 (4) RIPA regime as a whole.

The claimants have applied to the European Court of Human Rights (ECtHR) for review of the Tribunal's judgments;[15] their application has been fast tracked by the Court and was communicated to the British government in November 2015. It is anticipated that the case will be heard jointly with similar claims made in *Big Brother Watch and Others v. the United Kingdom*,[16] communicated on 9 January 2014, and *The Bureau of Investigative Journalism v. the United Kingdom*,[17] communicated on 15 January 2015.

The Investigatory Powers Bill, November 2015 to present

On 4 November 2015, the British Home Secretary, Theresa May, announced the publication of the Draft Investigatory Powers Bill, and the establishment of a Joint Committee to scrutinise the Bill.[18] The Draft Investigatory Powers Bill was designed to fulfil the objective identified by the Intelligence and Security Committee in its March 2015 report, namely the overhaul of the existing legal framework underpinning interception and communications surveillance by the police and intelligence agencies.[19] The Bill is intended to replace both Part I of RIPA, which currently regulates interception, and the Data Retention and Investigatory

---

[12] Anderson, D. (2015), *A question of trust: Report of the Investigatory Powers Review*, June 2015, p. 8, available at http://tinyurl.com/obodyky.
[13] Anderson, D. (2015), *A question of trust: Report of the Investigatory Powers Review*, June 2015, p. 269, available at http://tinyurl.com/obodyky.
[14] United Kingdom, Investigatory Powers Tribunal, *Liberty & Others v. the Security Service, SIS, GCHQ*, IPT/13/77/H, 22 June 2015, available at www.ipt-uk.com/docs/Final_Liberty_Ors_Open_Determination_Amended.pdf.
[15] ECtHR, *10 Human Rights Organisations v. United Kingdom*, No. 24960/15, Communicated 24 November 2015, available at http://hudoc.echr.coe.int/eng?i=001-159526.
[16] ECtHR, *Big Brother Watch v. United Kingdom*, No. 58170/13, Communicated 9 January 2014, available at http://hudoc.echr.coe.int/eng?i=001-140713.
[17] ECtHR, *The Bureau of Investigative Journalism v. the United Kingdom*, No. 62322/14, Communicated 5 January 2015, available at http://hudoc.echr.coe.int/eng?i=001-150946.
[18] United Kingdom, HM Home Office (2015), "Home Secretary introduces draft Investigatory Powers Bill", 4 November 2015, available at www.gov.uk/government/news/home-secretary-introduces-draft-investigatory-powers-bill.
[19] See United Kingdom, HM Home Office (2015), *Draft Investigatory Powers Bill*, 4 November 2015, available at www.gov.uk/government/uploads/system/uploads/attachment_data/file/473770/Draft_Investigatory_Powers_Bill.pdf.

Powers Act 2014 (DRIPA),[20] which was emergency legislation that will be repealed on 31 December 2016. The Bill contains powers related to targeted and bulk interception, targeted and bulk "equipment interference", retention and acquisition of communications data and "internet connection records", acquisition of communications data in bulk, and retention and examination of bulk personal datasets.[21] It also sets out a new oversight regime which will replace the existing oversight commissioners with a single new commissioner, the Investigatory Powers Commissioner. The Investigatory Powers Commissioner, a senior judge, will be supported by a number of Judicial Commissioners undertaking either authorisation or oversight and inspection functions. The Bill gives the Judicial Commissioners a role in approving surveillance warrants authorized by the Secretary of State.

Following the publication of the Draft Bill, the Joint Committee established to review the Bill took oral evidence from 59 people, and received 1,500 pages of written submissions.[22] Three other Committees, including the Joint Committee on Human Rights,[23] the Science and Technology Committee,[24] and the Intelligence and Security Committee,[25] all considered the Draft Bill during this time. With the exception of the Joint Committee on Human Rights, which is yet to report, the Committees raised concerns about the Draft Bill, with the Intelligence and Security Committee notably recommending the deletion of particular bulk powers from the legislation, and the introduction of "an entirely new part dedicated to overarching privacy protections".[26]

On 1 March 2016, the Investigatory Powers Bill was formally introduced into the House of Commons, with only few minor changes having been incorporated to reflect the Committees' recommendations.[27] The Bill has recently been scrutinised by a Public Bill Committee, charged with debating each clause and reporting any amendments to the House of Commons for further debate.[28] The Committee held examination sessions until the beginning of May

[20] United Kingdom, HM Government (2014), *Data Retention and Investigatory Powers Act 2014*, 17 July 2014, available at www.legislation.gov.uk/ukpga/2014/27.

[21] The definition of internet connection records can be found in Section 54 (6) of the Bill, namely communications data which "(a) may be used to identify, or assist in identifying, a telecommunications service to which a communication is transmitted by means of a telecommunication system for the purpose of obtaining access to, or running, a computer file or computer program, and
(b) comprises data generated or processed by a telecommunications operator in the process of supplying the telecommunications service to the sender of the communication (whether or not a person)".

[22] United Kingdom, Joint Committee on the Draft Investigatory Powers Bill (2016), *Draft Investigatory Powers Bill: Report*, 11 February 2016, available at www.publications.parliament.uk/pa/jt201516/jtselect/jtinvpowers/93/93.pdf.

[23] United Kingdom, Joint Committee on Human Rights (2016), "Investigatory Powers draft Legislative Scrutiny", April 2016, available at www.parliament.uk/business/committees/committees-a-z/joint-select/human-rights-committee/legislative-scrutiny/parliament-2015/investigatory-powers-draft-bill/.

[24] United Kingdom, House of Commons Science and Technology Committee (2016), *Investigatory Powers Bill: technology issues*, 1 February 2016, available at www.publications.parliament.uk/pa/cm201516/cmselect/cmsctech/573/573.pdf.

[25] United Kingdom, Intelligence and Security Committee of Parliament (2016), *Report on the draft Investigatory Powers Bill*, 9 February 2016, available at http://tinyurl.com/jsav59n.

[26] United Kingdom, Intelligence and Security Committee of Parliament (2016), "Report on the draft Investigatory Powers Bill – Press release", 9 February 2016, available at http://tinyurl.com/jmav2ds.

[27] United Kingdom, HM Home Office (2016), *Investigatory Powers Bill*, 1 March 2016, available at www.publications.parliament.uk/pa/bills/cbill/2015-2016/0143/16143.pdf.

[28] United Kingdom, UK Parliament (2016), 'House of Commons Public Bill Committee on the Investigatory Powers Bill 2015-16', available at http://services.parliament.uk/bills/2015-16/investigatorypowers/committees/houseofcommonspublicbillcommitteeontheinvestigatorypowersbill201516.html.

2016 and has now reported the Bill to the House with amendments.[29] The Bill has gone through the House of Commons and was last debated in Second Reading in the House of Lords on 27 June 2016.[30] The latest version of the Bill was published on 8 June 2016.[31] It is not expected that the Bill will be enacted until the end of 2016.[32]

MPs agreed a carry-over motion on 15 March 2016 which allows proceedings on the Bill to be resumed in the 2016-17 session of Parliament.

***Privacy International & Others v. the Foreign Secretary and GCHQ*, judgement of 12 February 2016**

Privacy International, in collaboration with seven internet and communications service providers from around the world, filed a claim in May 2014 against GCHQ and the Secretary of State for Foreign Affairs, alleging the unlawful use by GCHQ of "hacking" or "computer network exploitation" techniques.[33] The claim was stayed pending the resolution of the *Liberty* cases (see above). The claim asserted, inter alia, that GCHQ's activities were unlawful under Section 10 of the Computer Misuse Act 1990,[34] from which Section GCHQ did not enjoy an explicit exemption. In January 2015, Parliament adopted amendments to the Computer Misuse Act which asserted that other exemptions for GCHQ contained in the Act applied to Section 10. In February 2015, the Government promulgated a draft Equipment Interference Code of Practice,[35] which asserted the lawfulness of hacking techniques under existing provisions of the Intelligence Services Act 1994.[36] After the resolution of the *Liberty* cases in June 2015, the Privacy International claim proceeded. In February 2016, the Investigatory Powers Tribunal found that GCHQ hacking of mobiles, devices and computers was in fact lawful under British law. The Tribunal condoned GCHQ's use of a broad legal basis – the power to interfere with "property" under Section 5 of the Intelligence Services Act – to authorise hacking. It then concluded that adequate safeguards existed to prevent abuses of that power.

***Privacy International v. the Foreign Secretary and GCHQ*, ongoing**

In June 2015, Privacy International filed a further case in the Investigatory Powers Tribunal, in response to the revelation that GCHQ was acquiring and analysing bulk personal datasets.

---

[29] United Kingdom, UK Parliament, *Investigatory Powers Bill (as amended in Public Bill Committee)*, 4 May 2016, available at www.publications.parliament.uk/pa/bills/cbill/2015-2016/0172/160172.pdf.To see amendments made to the Bill in more detail, see the tracked changes version of the Bill here: www.parliament.uk/documents/commons-public-bill-office/2015-16/compared-bills/Investigatory-Powers-bill-160505.pdf.

[30] United Kingdom, UK Parliament, 'Investigatory Powers Bill: Remaining Stages', available at www.parliament.uk/business/news/2016/march/investigatory-powers-bill-commons-second-reading.

[31] United Kingdom, UK Parliament, *Investigatory Powers Bill*, 8 June 2016, available at: www.publications.parliament.uk/pa/bills/lbill/2016-2017/0040/17040.pdf.

[32] For the latest information, see: United Kingdom, UK Parliament, 'Investigatory Powers Bill 2015-16', available at http://services.parliament.uk/bills/2015-16/investigatorypowers.html.

[33] United Kingdom, Investigatory Powers Tribunal, *Privacy International and Greennet & Others v. the Secretary of State for Foreign and Commonwealth Affairs and GCHQ*, IPT 14/85/CH 14/120-126/CH, 12 February 2016, available at www.ipt-uk.com/docs/Privacy_Greennet_and_Sec_of_State.pdf.

[34] United Kingdom, HM Government (1990), *Computer Misuse Act 1990*, 29 June 1990, available at www.legislation.gov.uk/ukpga/1990/18.

[35] United Kingdom, HM Home Office (2015), *Equipment Interference: Code of Practice*, February 2015, available at www.gov.uk/government/uploads/system/uploads/attachment_data/file/401863/Draft_Equipment_Interference_Code_of_Practice.pdf.

[36] United Kingdom, HM Government (1994), *Intelligence Services Act 1994*, 26 May 1994, available at www.legislation.gov.uk/ukpga/1994/13.

The acquisition of such datasets has since been explicitly provided for in the Investigatory Powers Bill. In April 2016, the Tribunal ordered the disclosure of a significant tranche of documents possessed by the government concerning bulk personal datasets, including internal policy guidance.[37] The case is scheduled to proceed to hearing later this year.

[37] Privacy International (2016), 'Privacy International Releases Trove of Documents That Proves Staggering Reach of Surveillance Agencies', 20 April 2016, available at https://privacyinternational.org/node/853

1.2 International intelligence services cooperation

*FRANET contractors are requested to provide information, in 1 to 2 pages **maximum**, on the following two issues, drawing on a recent publication by Born, H., Leigh, I. and Wills, A. (2015), Making international intelligence cooperation accountable, Geneva, DCAF.*[38]

1. *It is assumed that in your Member State international cooperation between intelligence services takes place. Please describe the legal basis enabling such cooperation and any conditions that apply to it as prescribed by law. If the conditions are not regulated by a legislative act, please specify in what type of documents such cooperation is regulated (eg. internal guidance, ministerial directives etc.) and whether or not such documents are classified or publicly available.*
2. *Please describe whether and how the international cooperation agreements, the data exchanged between the services and any joint surveillance activities, are subject to oversight (executive control, parliament oversight and/or expert bodies) in your Member States.*

International intelligence services cooperation is vital to the United Kingdom's intelligence capabilities. In its submissions to the Investigatory Powers Tribunal in the case of *Liberty & Others*, the government asserted that "[i]ntelligence that foreign governments share with the intelligence services (on a strictly confidential basis) represents a significant proportion of the Intelligence Services' total store of intelligence on terrorists, organised criminals and others seeking to harm national security".[39]

The legal framework in the United Kingdom which presently governs international intelligence cooperation is relatively sparse. The legislative basis for intelligence cooperation is found in Sections 1 and 2 of the Security Service Act 1989,[40] which describe the functions of the Security Service ("MI5", the UK's domestic intelligence agency);[41] Sections 1 and 2 of the Intelligence Services Act 1994,[42] which describe the functions of the Secret Intelligence Service ("MI6", the UK's foreign intelligence service);[43] and Sections 3 and 4 of the Intelligence Services Act 1994,[44] which describe the functions of GCHQ (the UK's signals intelligence service). Each of these provisions endows on the respective intelligence service powers to obtain information so far as necessary for the proper discharge of its functions, which include broadly the protection of national security and economic well-being. The obtaining of information is subject to the oversight of a Director-General (MI5), Chief (MI6) or Director (GCHQ) responsible for ensuring that there are "arrangements" for securing that no information is obtained or disclosed by the Service except in accordance with the Service's functions.[45]

---

[38] http://www.dcaf.ch/Publications/Making-International-Intelligence-Cooperation-Accountable

[39] United Kingdom, Investigatory Powers Tribunal, *Liberty & Others v. the Security Service, SIS, GCHQ*, IPT/13/77/H, 5 December 2014, par. 15, available at www.ipt-uk.com/docs/IPT_13_168-173_H.pdf.

[40] United Kingdom, HM Government (1989), *Security Service Act 1989*, 27 April 1989, ss. 1-2, available at www.legislation.gov.uk/ukpga/1989/5.

[41] For more information, see: United Kingdom, MI5, www.mi5.gov.uk.

[42] United Kingdom, HM Government (1994), *Intelligence Services Act 1994*, 26 May 1994, ss. 1-2, available at www.legislation.gov.uk/ukpga/1994/13.

[43] For more information, see: United Kingdom, MI6, www.sis.gov.uk.

[44] United Kingdom, HM Government (1994), *Intelligence Services Act 1994*, 26 May 1994, ss. 3-4, available at www.legislation.gov.uk/ukpga/1994/13.

[45] United Kingdom, HM Government (1989), *Security Service Act 1989*, 27 April 1989, ss. 2 (1) and 4 (2) (a), available at www.legislation.gov.uk/ukpga/1989/5; United Kingdom, HM Government (1994), *Intelligence Services Act 1994*, 26 May 1994, s. 2 (1), available at www.legislation.gov.uk/ukpga/1994/13.

These legislative provisions relate to the obtaining and disclosure of "information", which while defined broadly does not seem to relate to cooperation beyond information sharing, for which there is no apparently legislative basis. However, "the term 'information' is a very broad one, and is capable of covering e.g. communications and communications data […] that a foreign intelligence agency may have obtained and passed to the Intelligence Services".[46] In fact, the term "information" is interpreted to cover intelligence derived from sources other than communications and communications data, including information derived from covert human intelligence sources or covert property searches.[47]In view of this broad term, it is possible for information derived from communications and communications themselves to be shared.

In addition to the abovenamed provisions, Section 19 (2) of the Counter-Terrorism Act 2008 states that "(i)nformation obtained by any of the intelligence services in connection with the exercise of any of its functions may be used by that service in connection with the exercise of any of its other functions".[48] Sections 19 (3) and (4) of the Act provide that information obtained by, respectively, MI5 and MI6 for the purposes of any of its functions "may be disclosed by it (a) for the purpose of the proper discharge of its functions; (b) in the interests of national security; (c) for the purpose of the prevention or detection of serious crime; or (d) for the purpose of any criminal proceedings". There is a similar provision, but limited to (a) and (d), relating to GCHQ in Section 19 (5) of the Act. Regarding data obtained by foreign intelligence services and shared with British intelligence services, the Investigatory Powers Tribunal, in the case of *Liberty & Ors v. The Security Services & Ors*, has summarised the situation as being one in which "any request for, or receipt of, intercept or communications data pursuant [international intelligence sharing arrangements] is ordinarily subject to the same safeguards as in a case where intercept or communication data are obtained directly" by the government.[49] Therefore, there is a data flow irrespective of purpose for which the data are initially obtained.

With respect to the "arrangements" regarding the handling of material obtained from and disclosed to foreign intelligence organisations, such arrangements are not publicly available. This feature was at the heart of the litigation brought by Liberty and other NGOs against the Security and Intelligence Services in the Investigatory Powers Tribunal. In its judgment of 5 December 2014, the Tribunal concluded that it was "satisfied that in the field of intelligence sharing it is not to be expected that rules need to be contained in statute […] or even in a code", but rather that it is sufficient that

> "i) Appropriate rules or *arrangements* exist and are publicly known and confirmed to exist, with their content sufficiently signposted, such as to give an *adequate indication* of it […];
> ii) They are subject to proper oversight".[50]

---

[46] United Kingdom, Investigatory Powers Tribunal, *Liberty & Others v. the Security Service, SIS, GCHQ*, IPT/13/77/H, 5 December 2014, par. 18 (ix), available at www.ipt-uk.com/docs/IPT_13_168-173_H.pdf.

[47] United Kingdom, Investigatory Powers Tribunal, *Liberty & Others v. the Security Service, SIS, GCHQ*, IPT/13/77/H, 5 December 2014, par. 26, available at www.ipt-uk.com/docs/IPT_13_168-173_H.pdf.

[48] United Kingdom, HM Government (2008), *Counter-Terrorism Act 2008*, 26 November 2008, s. 19 (2), available at www.legislation.gov.uk/ukpga/2008/28.

[49] United Kingdom, Investigatory Powers Tribunal, *Liberty & Others v. the Security Service, SIS, GCHQ*, IPT/13/77/H, 5 December 2014, par. 53, available at www.ipt-uk.com/docs/IPT_13_168-173_H.pdf.

[50] United Kingdom, Investigatory Powers Tribunal, *Liberty & Others v. the Security Service, SIS, GCHQ*, IPT/13/77/H, 5 December 2014, par. 41, available at www.ipt-uk.com/docs/IPT_13_168-173_H.pdf.

In the course of the *Liberty* case before the Investigatory Powers Tribunal, the government confirmed the existence of internal guidance, training procedures and "below the waterline" (i.e. confidential) arrangements between the UK intelligence services and their foreign partners, applicable to the exchange of information contained in or derived from intercepted communications or communications data. In addition, a Disclosure was made by the government in the course of proceedings which the Tribunal published in full in its judgement of 5 December 2014; the Disclosure concerned the conditions under which "unanalysed intercepted communications (and associated communications data)" could be requested by the British intelligence services from a foreign intelligence agency.[51] The Disclosure stipulates that when such material is requested, either a relevant interception warrant has already been issued, or making the request without a warrant would not amount to a deliberate circumvention of RIPA (for example, because it is not technically feasible to obtain the communications via RIPA interception). In all circumstances, it must be necessary and proportionate for the intelligence services to obtain the communications.

With respect to the requirement that such arrangements are subject to adequate oversight, to the extent to which intelligence cooperation and information sharing is considered part of the exercise of functions by the relevant intelligence agencies, it is subject to the same oversight as that applicable to the exercise of those functions. That oversight includes the Intelligence and Security Committee of Parliament, and the oversight afforded by the Interception of Communications Commissioner under Section 57 (1) of RIPA, who is independent from the government and the intelligence services.

There has been no further information placed into the public domain about the existence or substance of internal guidance or arrangements applicable to other forms of intelligence cooperation or information sharing. There is, however, in the public domain a series of agreements and memoranda of understanding, dating back as early as 1946, between the United Kingdom, United States, Australia, Canada and New Zealand, which are collectively known as the 'Five Eyes Agreement'.[52] The documents were classified until their transfer to the National Archives in 2010, and continue to govern arrangements between the particular countries in relation to the exchange of intelligence information relating to 'foreign' communications, defined by reference to countries other than the United States, the United Kingdom and the Commonwealth. There is no explicit statutory reference to the existence of the Agreement, nor to the oversight arrangements applicable thereto. However, to the extent that the Intelligence and Security Committee has general oversight over the activities of the intelligence agencies it is assumed that foreign intelligence cooperation would fall within its remit. International intelligence sharing does not appear to fall within the statutory remit of the Interception of Communications Commissioner's oversight functions. In his 2013 annual report, the Commissioner noted that he is asked to "review the consequent arrangements" regarding receipt of foreign intercept material, although it "may not be within [his] statutory remit".[53]

The Investigatory Powers Bill, pending in Parliament, does not appear to substantially alter or elaborate upon the statutory basis for intelligence cooperation, although it does contain numerous provisions relating to law enforcement cooperation under the auspices of mutual legal assistance processes. The absence of substantive reform to or regulation of intelligence

[51] United Kingdom, Investigatory Powers Tribunal, *Liberty & Others v. the Security Service, SIS, GCHQ*, IPT/13/77/H, 5 December 2014, par. 47, available at www.ipt-uk.com/docs/IPT_13_168-173_H.pdf.

[52] For more information, see: Privacy International, "The Five Eyes", available at www.privacyinternational.org/node/51.

[53] Excerpted in United Kingdom, Investigatory Powers Tribunal, *Liberty & Others v. the Security Service, SIS, GCHQ*, IPT/13/77/H, 5 December 2014, par. 24, available at www.ipt-uk.com/docs/IPT_13_168-173_H.pdf.

sharing, in particular, was the subject of some criticism by the ISC which, in examining the Draft Investigatory Powers Bill, emphasised that "the proportion of intercept material obtained from international partners is such that it is not appropriate to exclude it from legislation which purports to cover interception". [54] The Joint Committee (specifically established to analyse the Draft Bill) also noted this significant omission and called for "more safeguards for the sharing of intelligence with overseas agencies on the face of the Bill", which should necessarily "address concerns about potential human rights violations in other countries that information can be shared with".[55] In response, the Government introduced a provision restricting UK authorities from requesting a foreign intelligence agency from carrying out interception of communications in the absence of a warrant.[56]

[54] United Kingdom, Intelligence and Security Committee of Parliament (2016), *Report on the draft Investigatory Powers Bill*, 9 February 2016, p. 12, available at http://tinyurl.com/jsav59n.
[55] United Kingdom, Joint Committee on the Draft Investigatory Powers Bill (2016), *Draft Investigatory Powers Bill: Report*, 11 February 2016, p. 17, available at www.publications.parliament.uk/pa/jt201516/jtselect/jtinvpowers/93/93.pdf.
[56] United Kingdom, HM Home Office (2016), *Investigatory Powers Bill: Government Response to Pre-Legislative Scrutiny*, March 2016, p. 62, available www.gov.uk/government/uploads/system/uploads/attachment_data/file/504174/54575_Cm_9219_WEB.PDF; United Kingdom, HM Home Office (2016), *Investigatory Powers Bill*, 1 March 2016, s. 47, available at www.publications.parliament.uk/pa/bills/cbill/2015-2016/0143/16143.pdf

1.3 Access to information and surveillance

*FRANET contractors are requested to summarise, in 1 to 2 pages **maximum**, the legal framework in their Member State in relation to surveillance and access to information.*
Please refer to the Global Principles on National Security and the Right to Information (the Tshwane Principles)[57] (in particular Principle 10 E. – Surveillance) and describe the relevant national legal framework in this context. FRANET contractors could in particular answer the following questions:

1. *Does a complete exemption apply to surveillance measures in relation to access to information?*
2. *Do individuals have the right to access information on whether they are subject to surveillance?*

Access to information in the United Kingdom is regulated by the Freedom of Information Act 2000,[58] which stipulates the conditions under which individuals can apply to government departments for access to information. However, in Section 84 of the Act, which stipulates the definitions of the terms used therein, "government department" is defined so as to exclude the Security Services (MI5), the Secret Intelligence Service (MI6) and the Government Communications Headquarters (GCHQ). As a result, the intelligence services are not a "public authority" to which the Act applies, by virtue of Schedule 1 of the Act, and therefore enjoy a blanket exemption from access to information processes. Furthermore, the Security Service Act 1989 and the Intelligence Services Act 1994 both place a statutory obligation on the respective directors/chiefs of the intelligence agencies to ensure that no information is disclosed by the services except so far as it is necessary for the proper discharge of their function.[59]

The right of individuals to request access to data relating specifically to them, enshrined in the Data Protection Act 1998 (DPA),[60] is subject to exemptions for the safeguarding of national security, which are applied on a case by case basis. In addition, the Secretary of State can, in accordance with Section 28 (1) of the Act, certify the exemption of certain authorities from particular parts of the Act. The Secretary of State has indeed issued such certificates exempting GCHQ, MI6[61] and MI5[62] from the data protection principles and Parts II (Rights of data subjects), III (Notification by data controllers), V (Enforcement) and Section 55 (Unlawful obtaining of personal data) of the DPA. The data protection principles are set out in Schedule 1 of the DPA, namely: personal data shall be 1) processed fairly and lawfully; 2) obtained for specified and lawful purposes; 3) adequate, relevant and not excessive in relation to the purposes for which they are processed; 4) accurate; 5) not be kept for longer than is necessary; 6) processed in accordance with the rights of data subjects; 7) measures shall be taken against unauthorised or unlawful processing of personal data; and 8) not be transferred to a country or territory outside the European Economic Area unless that country or territory

[57] http://www.right2info.org/exceptions-to-access/national-security/global-principles#section-10
[58] United Kingdom, HM Government (2000), *Freedom of Information Act 2000*, 30 November 2000, available at www.legislation.gov.uk/ukpga/2000/36.
[59] United Kingdom, HM Government (1989), *Security Service Act 1989*, 27 April 1989, s. 2 (2) (a), available at www.legislation.gov.uk/ukpga/1989/5; United Kingdom, HM Government (1994), *Intelligence Services Act 1994*, 26 May 1994, ss. 2 (2) (a) and 4 (2) (a), available at www.legislation.gov.uk/ukpga/1994/13.
[60] United Kingdom, HM Government (1998), *Data Protection Act 1998*, 16 July 1998, available at www.legislation.gov.uk/ukpga/1998/29.
[61] GCHQ and MI6 are dealt with jointly; certificate available at http://amberhawk.typepad.com/files/blog-s.28-straw-certificate-gchq-sis-no.-2-2001.pdf.
[62] Certificate available at http://amberhawk.typepad.com/files/blog-s.28-blunkett-certificate-security-service-2001.pdf.

ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.[63]

The Information Commissioner's Office (ICO), who has oversight over the implementation of and compliance with the Data Protection Act, has limited powers of oversight with respect to the exercise of exemptions in response to requests for access to data, as prescribed by a 2014 memorandum of understanding (MoU) on national security cases (Data Protection Act) between the Secretary of State for Justice and the Information Commissioner. The MoU provides guidelines for cooperation between the Information Commissioner's Office (ICO) and the security services.[64] The MoU relates to the ICO's enforcement powers under Sections 42 (Request for assessment) and 43 (Information notices) of the Act, with respect to instances in which the Section 28 exemption for national security cases is relied upon in response to subject access requests. The MoU circumscribes the extent and scope of information required to be provided by the security services in response to requests for information from the ICO. It explicitly endorses the Commissioner's power to assess whether the relevant exemptions justifying nondisclosure and/or the 'neither confirm nor deny response' have been properly relied on (powers under Part V of the DPA).[65] However, it sets out specific steps to be taken due to the sensitive nature of cases related to national security.[66] Specifically, the MoU emphasises that cases should as much as possible be resolved "through dialogue and correspondence between the Commissioner and the relevant Department" and that, in the majority of cases, "a reasoned explanation together with any relevant background information […] will usually be sufficient to satisfy the Commissioner that the relevant exemptions have been properly relied on […] without disclosing to the Commissioner the detailed content of the withheld information or personal data […] .[67] In the exceptional cases that this reasoned explanation is not enough, the MoU recognises that it might be necessary for the Commissioner to be granted confidential access to the withheld information or data, and the process and requirements to access these is set out in the MoU.[68] The MoU further states that the ICO's statutory enforcement powers (serving the security services with a formal information notice under Section 43 or enforcement notice under Section 40) should only be used if the case was not resolved through dialogue, and even in that case the MoU stipulates that there should be further notification to the security services and consultation.[69] The consequences for the data subject's right to access the information or personal data are that the Commissioner cannot disclose either the reasoned explanation or the withheld information unless the relevant security services consent to the disclosure or all appeal proceedings have

[63] United Kingdom, HM Government (1998), *Data Protection Act 1998*, 16 July 1998, sch. 1, available at www.legislation.gov.uk/ukpga/1998/29.
[64] United Kingdom, Ministry of Justice (2014), 'Memorandum of understanding between on National Security Cases (FOIA and EIR)', January 2014, available at https://ico.org.uk/media/about-the-ico/documents/1042532/mou-national-security-cases-dpa.pdf.
[65] United Kingdom, Ministry of Justice (2014), 'Memorandum of understanding between on National Security Cases (FOIA and EIR)', January 2014, par. 6, available at https://ico.org.uk/media/about-the-ico/documents/1042532/mou-national-security-cases-dpa.pdf.
[66] United Kingdom, Ministry of Justice (2014), 'Memorandum of understanding between on National Security Cases (FOIA and EIR)', January 2014, par. 7, available at https://ico.org.uk/media/about-the-ico/documents/1042532/mou-national-security-cases-dpa.pdf.
[67] United Kingdom, Ministry of Justice (2014), 'Memorandum of understanding between on National Security Cases (FOIA and EIR)', January 2014, par. 11, available at https://ico.org.uk/media/about-the-ico/documents/1042532/mou-national-security-cases-dpa.pdf.
[68] United Kingdom, Ministry of Justice (2014), 'Memorandum of understanding between on National Security Cases (FOIA and EIR)', January 2014, par. 12, available at https://ico.org.uk/media/about-the-ico/documents/1042532/mou-national-security-cases-dpa.pdf.
[69] United Kingdom, Ministry of Justice (2014), 'Memorandum of understanding between on National Security Cases (FOIA and EIR)', January 2014, paras. 13-14 and 25-29, available at https://ico.org.uk/media/about-the-ico/documents/1042532/mou-national-security-cases-dpa.pdf.

been exhausted.[70] Overall, in practical terms, the MoU seems to restrict the ICO's powers significantly and reduces the data subject's right to access to a mere right to request the Commissioner to verify the relevant security services' justifications for withholding information or personal data.

The case that led to the adoption of the MoU is *R. v. Information Tribunal*.[71] In this case, the Secretary of State had applied for judicial review of a decision of the National Security Appeals Panel allowing the appeal of the Information Commissioner under Section 28 (4) of the DPA against a certificate signed by the Secretary of State on the basis of Section 28 (2). In the case, an individual (X) had, on the basis of Section 7, applied to the Immigration and Nationality Directorate of the Home Department for information on any personal data held in respect of him. Dissatisfied with the response, X had requested the Information Commissioner to intervene. The Commissioner treated this as a "request for assessment" under Section 42 and wrote to the Home Department asking for disclosure of the withheld information. The Home Department replied that the national security exemption under Section 28 applied, that the nature of the disclosure given to X was in conformity with the government's policy with regard to matters involving security and intelligence agencies (namely, to "neither confirm or deny" the existence of information) and that the information would not be made available to the Commissioner. The Commissioner served a preliminary information notice on the Home Department followed by an information notice under Section 43. The Secretary of State subsequently signed a certificate under Section 28 (2) stating that an exemption was being claimed on the ground of national security, against which the Commissioner appealed to the tribunal. The Secretary argued that the Commissioner had no statutory powers that he could exercise under Part V of the DPA which could entitle him to second-guess a ministerial certificate. The tribunal held that, as both the Commissioner and the Secretary had roles to play within the context of Section 28 exemptions, the Commissioner's role could not be excluded on the ground of national security and that, as the Secretary had fundamentally misdirected himself as to the law, the certificate was liable to be quashed. Section 51 (1) entitled the Commissioner to check whether an exemption under Section 28 had been properly claimed.

There is no obligation on the intelligence services to notify individuals that they have been subjected to surveillance. The absence of notification is counter-balanced by a system for remedying complaints regarding unlawful activity whereby individuals do not need to establish that they have been subject to surveillance in order to have an admissible claim regarding unlawful activity. According to the Investigatory Powers Tribunal Rules 2000,[72] individuals are entitled to have their claim of unlawful surveillance heard by the Investigatory Powers Tribunal, and can rely on any evidence, including evidence that would not be admissible in a court of law (Rule 11).

However, the Tribunal's Rules greatly restrict what information can be disclosed to a claimant in the course of their complaint. Rule 6 (2) provides that the Tribunal can withhold any information or document disclosed or provided during proceedings, and does not need to disclose to the claimant the fact that an oral hearing has taken place. The Tribunal is, in any event, under no obligation to hold oral hearings (Rule 9 (2)). Complainants will be notified of the outcome of the case. If a determination is made in favour of the complainant the findings

[70] United Kingdom, Ministry of Justice (2014), 'Memorandum of understanding between on National Security Cases (FOIA and EIR)', January 2014, par. 18, available at https://ico.org.uk/media/about-the-ico/documents/1042532/mou-national-security-cases-dpa.pdf.

[71] United Kingdom, Divisional Court, *R. (on the application of Secretary of State for the Home Department) v Information Tribunal*, [2006] EWHC 2958 (Admin), 23 November 2006. Case attached to final submission.

[72] United Kingdom, HM Government (2000), *The Investigatory Powers Tribunal Rules 2000*, 28 September 2000, available at www.legislation.gov.uk/uksi/2000/2665.

of fact must be provided. Complainants are not however entitled to be informed of the reasons of decisions not made in their favour (Rule 13).

1.4 Update the FRA report

FRANET contractors are requested to provide up-to-date information based on the FRA report on Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU – mapping Member Stat by…es' legal framework.

*Please take into account the **Bibliography/References** (p. 79 f. of the FRA report), as well as the **Legal instruments index – national legislation** (p. 88 f. the FRA report) when answering the questions.*

Introduction

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

The UK is mentioned on page 7. The references in the text on page 7 are accurate.

1 Intelligence services and surveillance laws

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

1.1 Intelligence services

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

The UK is not explicitly mentioned. It is not necessary to mention the UK for the relevance of FRA's analysis under this section.

1.2 Surveillance measures

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

The UK is mentioned on page 18. The reference is correct. It might also be useful, in addition, to refer to the legislative process underway to replace RIPA (the Investigatory Powers Bill: United Kingdom, HM Home Office (2016), *Investigatory Powers Bill*, 1 March 2016,

available at www.publications.parliament.uk/pa/bills/cbill/2015-2016/0143/16143.pdf)[73] as a result of the report of the Intelligence and Security Committee.[74]

1.3 Member States' laws on surveillance

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

The UK is mentioned on pages 23, 24 and 26. The references are correct.[75] However, with regard to page 23 (signals intelligence), reference should be made to the new Investigatory Powers Bill that will replace RIPA (probably by the end of 2016).[76] This Bill explicitly uses the term "bulk interception" and sets out a new statutory regime with regard to bulk interception warrants.[77] The Bill did recently undergo its second reading in the UK Parliament House of Lords,[78] and therefore amendments to it are still possible. This should be taken into account in the following sections, when referring to the Bill "in its current form".

FRA key findings

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

The UK is not explicitly mentioned. It is not necessary to mention the UK for the relevance of FRA's analysis under this section.

2 Oversight of intelligence services

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

---

[73] Latest version: United Kingdom, UK Parliament, *Investigatory Powers Bill*, 8 June 2016, available at www.publications.parliament.uk/pa/bills/lbill/2016-2017/0040/17040.pdf.

[74] Namely, United Kingdom, Intelligence and Security Committee of Parliament (ISC) (2015), *Privacy and Security: A modern and transparent legal framework*, 12 March 2015, p. 2, available at http://tinyurl.com/zg95dez.

[75] Minor remark: The text of the FRA Report refers to Sections "8.5", "8.4" and "5.3" but these are "8 (5)", "8 (4)" and "5 (3)".

[76] United Kingdom, HM Home Office (2016), *Investigatory Powers Bill*, 1 March 2016, available at http://www.publications.parliament.uk/pa/bills/cbill/2015-2016/0143/16143.pdf. Latest version: United Kingdom, UK Parliament, *Investigatory Powers Bill*, 8 June 2016, available at www.publications.parliament.uk/pa/bills/lbill/2016-2017/0040/17040.pdf.

[77] United Kingdom, UK Parliament, *Investigatory Powers Bill*, 8 June 2016, part 6, available at www.publications.parliament.uk/pa/bills/lbill/2016-2017/0040/17040.pdf

[78] United Kingdom, UK Parliament, "Investigatory Powers Bill 2015-16", available at http://services.parliament.uk/bills/2015-16/investigatorypowers.html.

The UK is mentioned on page 31. The references are correct.

As mentioned above, the Investigatory Powers Bill will replace RIPA by the end of 2016. In its current form, the Bill will abolish the IOCCO and replace it with the Investigatory Powers Commissioner.[79]

2.1 Executive control

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

The UK is mentioned on page 33. The references are correct. If the Investigatory Powers Bill is accepted in its current form, the correct references will be Sections 17, 91, 121, 138 and 156 for footnote 214, and Section 194 for footnote 215.

2.2 Parliamentary oversight

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

The UK is not explicitly mentioned. It is not necessary to mention the UK for the relevance of FRA's analysis under this section.

2.2.1 Mandate

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

The UK is mentioned on pages 37-39. The references are correct. Similar to above, a reference to the Investigatory Powers Bill underway to replace RIPA might be useful at the end of the paragraph on page 38.

2.2.2 Composition

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*

[79] United Kingdom, UK Parliament, *Investigatory Powers Bill*, 8 June 2016, s. 215, available at www.publications.parliament.uk/pa/bills/lbill/2016-2017/0040/17040.pdf

3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

The UK is mentioned on page 39. The reference is correct.[80]

2.2.3 Access to information and documents

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

The UK is mentioned on page 40. The reference is correct.

2.2.3 Reporting to parliament

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

The UK is mentioned on page 41. The reference is correct.

2.3 Expert oversight

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

2.3.1 Specialised expert bodies

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

The UK is mentioned on page 45. The references are correct.[81] If the Investigatory Powers Bill is accepted in its current form, the Intelligence Services Commissioner and the Interception of Communications Commissioners will be replaced by the Investigatory Powers

[80] Minor remark: the exact reference to the nomination by the Prime Minister is in Section 1 (4) (a) of the Justice and Security Act.
[81] Minor remark on footnote 344: the correct page is p. 120.

Commissioner.[82] As mentioned above under Section 2, in July 2015 IOCCO published a report updating its March 2015 report. Mainly, the report provides details of the serious communications data errors that were reported to IOCCO in 2014 and recommendations given.[83]

2.3.2 Data protection authorities

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

The UK is mentioned on page 47. The reference is correct. In addition, if the Investigatory Powers Bill is accepted in its current form, the Information Commissioner will be given some powers, namely to "audit compliance with requirements or restrictions imposed by virtue of Part 4 [retention of communications data] in relation to the integrity, security or destruction of data retained by virtue of that Part" (Section 219 of the Bill). It will be possible to retain data on the basis of national security (Section 83 (1) c.f. Section 58 (7) (a)) but the ICO's specific powers in relation to this are not yet clear at this stage of the legislative process.

The right of individuals to request access to data relating specifically to them, enshrined in the Data Protection Act 1998 (DPA),[84] is subject to exemptions for the safeguarding of national security, which are applied on a case by case basis. In addition, the Secretary of State can, in accordance with Section 28 (1) of the Act, certify the exemption of certain authorities from particular parts of the Act. The Secretary of State has indeed issued such certificates exempting GCHQ, MI6[85] and MI5[86] from the data protection principles and Parts II (Rights of data subjects), III (Notification by data controllers), V (Enforcement) and Section 55 (Unlawful obtaining of personal data) of the DPA. The data protection principles are set out in Schedule 1 of the DPA, namely: personal data shall be 1) processed fairly and lawfully; 2) obtained for specified and lawful purposes; 3) adequate, relevant and not excessive in relation to the purposes for which they are processed; 4) accurate; 5) not be kept for longer than is necessary; 6) processed in accordance with the rights of data subjects; 7) measures shall be taken against unauthorised or unlawful processing of personal data; and 8) not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.[87]

The Information Commissioner's Office (ICO), who has oversight over the implementation of and compliance with the Data Protection Act, has limited powers of oversight with respect to

[82] United Kingdom, UK Parliament, *Investigatory Powers Bill*, 8 June 2016, s. 215, available at www.publications.parliament.uk/pa/bills/lbill/2016-2017/0040/17040.pdf.

[83] United Kingdom, Interception of Communications Commissioner (IOCCO) (2015), *Half-yearly report of the Interception of Communications Commissioner*, No. HC 308 SG/2015/105, London, July 2015, pp. 15-43, available at http://www.iocco-uk.info/docs/2015%20Half-yearly%20report%20(web%20version).pdf.

[84] United Kingdom, HM Government (1998), *Data Protection Act 1998*, 16 July 1998, available at www.legislation.gov.uk/ukpga/1998/29.

[85] GCHQ and MI6 are dealt with jointly; certificate available at http://amberhawk.typepad.com/files/blog-s.28-straw-certificate-gchq-sis-no.-2-2001.pdf.

[86] Certificate available at http://amberhawk.typepad.com/files/blog-s.28-blunkett-certificate-security-service-2001.pdf.

[87] United Kingdom, HM Government (1998), *Data Protection Act 1998*, 16 July 1998, sch. 1, available at www.legislation.gov.uk/ukpga/1998/29.

the exercise of exemptions in response to requests for access to data, as prescribed by a 2014 memorandum of understanding (MoU) on national security cases (Data Protection Act) between the Secretary of State for Justice and the Information Commissioner. The MoU provides guidelines for cooperation between the Information Commissioner's Office (ICO) and the security services.[88] The MoU relates to the ICO's enforcement powers under Sections 42 (Request for assessment) and 43 (Information notices) of the Act, with respect to instances in which the Section 28 exemption for national security cases is relied upon in response to subject access requests. The MoU circumscribes the extent and scope of information required to be provided by the security services in response to requests for information from the ICO. It explicitly endorses the Commissioner's power to assess whether the relevant exemptions justifying nondisclosure and/or the 'neither confirm nor deny response' have been properly relied on (powers under Part V of the DPA).[89] However, it sets out specific steps to be taken due to the sensitive nature of cases related to national security.[90] Specifically, the MoU emphasizes that cases should as much as possible be resolved "through dialogue and correspondence between the Commissioner and the relevant Department" and that, in the majority of cases, "a reasoned explanation together with any relevant background information […] will usually be sufficient to satisfy the Commissioner that the relevant exemptions have been properly relied on […] without disclosing to the Commissioner the detailed content of the withheld information or personal data […] .[91] In the exceptional cases that this reasoned explanation is not enough, the MoU recognizes that it might be necessary for the Commissioner to be granted confidential access to the withheld information or data, and the process and requirements to access these is set out in the MoU.[92] The MoU further states that the ICO's statutory enforcement powers (serving the security services with a formal information notice under Section 43 or enforcement notice under Section 40) should only be used if the case was not resolved through dialogue, and even in that case the MoU stipulates that there should be further notification to the security services and consultation.[93] The consequences for the data subject's right to access the information or personal data are that the Commissioner cannot disclose either the reasoned explanation or the withheld information unless the relevant security services consent to the disclosure or all appeal proceedings have been exhausted.[94] Overall, in practical terms, the MoU seems to restrict the ICO's powers significantly and reduces the data subject's right to access to a mere right to request the Commissioner to verify the relevant security services' justifications for withholding information or personal data.

---

[88] United Kingdom, Ministry of Justice (2014), 'Memorandum of understanding between on National Security Cases (FOIA and EIR)', January 2014, available at https://ico.org.uk/media/about-the-ico/documents/1042532/mou-national-security-cases-dpa.pdf.

[89] United Kingdom, Ministry of Justice (2014), 'Memorandum of understanding between on National Security Cases (FOIA and EIR)', January 2014, par. 6, available at https://ico.org.uk/media/about-the-ico/documents/1042532/mou-national-security-cases-dpa.pdf.

[90] United Kingdom, Ministry of Justice (2014), 'Memorandum of understanding between on National Security Cases (FOIA and EIR)', January 2014, par. 7, available at https://ico.org.uk/media/about-the-ico/documents/1042532/mou-national-security-cases-dpa.pdf.

[91] United Kingdom, Ministry of Justice (2014), 'Memorandum of understanding between on National Security Cases (FOIA and EIR)', January 2014, par. 11, available at https://ico.org.uk/media/about-the-ico/documents/1042532/mou-national-security-cases-dpa.pdf.

[92] United Kingdom, Ministry of Justice (2014), 'Memorandum of understanding between on National Security Cases (FOIA and EIR)', January 2014, par. 12, available at https://ico.org.uk/media/about-the-ico/documents/1042532/mou-national-security-cases-dpa.pdf.

[93] United Kingdom, Ministry of Justice (2014), 'Memorandum of understanding between on National Security Cases (FOIA and EIR)', January 2014, paras. 13-14 and 25-29, available at https://ico.org.uk/media/about-the-ico/documents/1042532/mou-national-security-cases-dpa.pdf.

[94] United Kingdom, Ministry of Justice (2014), 'Memorandum of understanding between on National Security Cases (FOIA and EIR)', January 2014, par. 18, available at https://ico.org.uk/media/about-the-ico/documents/1042532/mou-national-security-cases-dpa.pdf.

The case that led to the adoption of the MoU is *R. v. Information Tribunal*.[95] In this case, the Secretary of State had applied for judicial review of a decision of the National Security Appeals Panel allowing the appeal of the Information Commissioner under Section 28 (4) of the DPA against a certificate signed by the Secretary of State on the basis of Section 28 (2). In the case, an individual (X) had, on the basis of Section 7, applied to the Immigration and Nationality Directorate of the Home Department for information on any personal data held in respect of him. Dissatisfied with the response, X had requested the Information Commissioner to intervene. The Commissioner treated this as a "request for assessment" under Section 42 and wrote to the Home Department asking for disclosure of the withheld information. The Home Department replied that the national security exemption under Section 28 applied, that the nature of the disclosure given to X was in conformity with the government's policy with regard to matters involving security and intelligence agencies (namely, to "neither confirm or deny" the existence of information) and that the information would not be made available to the Commissioner. The Commissioner served a preliminary information notice on the Home Department followed by an information notice under Section 43. The Secretary of State subsequently signed a certificate under Section 28 (2) stating that an exemption was being claimed on the ground of national security, against which the Commissioner appealed to the tribunal. The Secretary argued that the Commissioner had no statutory powers that he could exercise under Part V of the DPA which could entitle him to second-guess a ministerial certificate. The tribunal held that, as both the Commissioner and the Secretary had roles to play within the context of Section 28 exemptions, the Commissioner's role could not be excluded on the ground of national security and that, as the Secretary had fundamentally misdirected himself as to the law, the certificate was liable to be quashed. Section 51 (1) entitled the Commissioner to check whether an exemption under Section 28 had been properly claimed.

2.4 Approval and review of surveillance measures

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

The UK is mentioned on pages 53, 55 and 56. The references are correct.

On page 53, if the Investigatory Powers Bill is accepted in its current form, the new provisions will be Sections 19, 96, 129, 146 and 164 for footnote 386. Additionally, the system would change as any warrant would, in addition, have to be approved by a judicial commissioner (as suggested by the Independent Reviewer of Terrorism Legislation on page 56).[96] On page 55, the new provision will be Section 127 for footnote 417.

On page 55, it might be useful to refer to the ISC's new report: *Report on the draft Investigatory Powers Bill*.[97] On page 10, for example, the ISC recommends deleting the

[95] United Kingdom, Divisional Court, *R. (on the application of Secretary of State for the Home Department) v Information Tribunal*, [2006] EWHC 2958 (Admin), 23 November 2006. Case attached to final submission.

[96] United Kingdom, UK Parliament, *Investigatory Powers Bill*, 8 June 2016, ss. 23, 102, 147, 165 and 188, available at www.publications.parliament.uk/pa/bills/lbill/2016-2017/0040/17040.pdf

[97] United Kingdom, Intelligence and Security Committee of Parliament (2016), *Report on the draft Investigatory Powers Bill*, 9 February 2016, available at http://tinyurl.com/jsav59n.

"confusing" category of "economic well-being".[98] This report builds upon the broader report *Privacy and Security: A modern and transparent legal framework* mentioned in the paragraph and scrutinises the draft Investigatory Powers Bill which was published in November 2015 (and since then replaced by the current Investigatory Powers Bill in Parliament).

FRA key findings

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

The UK is not explicitly mentioned. It is not necessary to mention the UK for the relevance of FRA's analysis under this section.

3 Remedies

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

The UK is mentioned on pages 59-60. The references are correct. As above, a reference to the Investigatory Powers Bill underway might be useful.

3.1 A precondition: obligation to inform and the right to access

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

The UK is mentioned on page 62. The reference is correct. In addition, the right of individuals to request access to data relating specifically to them, enshrined in the Data Protection Act 1998,[99] is subject to exemptions for the safeguarding of national security, which are applied on a case by case basis. In addition, the Secretary of State can, in accordance with Section 28 (1) of the Act, certify the exemption of certain authorities from particular parts of the Act. The Secretary of State has indeed issued such certificates exempting GCHQ, MI6[100] and MI5[101] from the data protection principles and Parts II (Rights of data subjects), III (Notification by data controllers), V (Enforcement) and Section 55 (Unlawful obtaining of

[98] This category is, however, still used in the Investigatory Powers Bill, for example in Section 18 (2) (c).

[99] United Kingdom, HM Government (1998), *Data Protection Act 1998*, 16 July 1998, available at www.legislation.gov.uk/ukpga/1998/29.

[100] GCHQ and MI6 are dealt with jointly; certificate available at http://amberhawk.typepad.com/files/blog-s.28-straw-certificate-gchq-sis-no.-2-2001.pdf.

[101] Certificate available at http://amberhawk.typepad.com/files/blog-s.28-blunkett-certificate-security-service-2001.pdf.

personal data) of the DPA. The data protection principles are set out in Schedule 1 of the DPA, namely: personal data shall be 1) processed fairly and lawfully; 2) obtained for specified and lawful purposes; 3) adequate, relevant and not excessive in relation to the purposes for which they are processed; 4) accurate; 5) not be kept for longer than is necessary; 6) processed in accordance with the rights of data subjects; 7) measures shall be taken against unauthorised or unlawful processing of personal data; and 8) not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.[102]

The Information Commissioner's Office (ICO), who has oversight over the implementation of and compliance with the Data Protection Act, has limited powers of oversight with respect to the exercise of exemptions in response to requests for access to data, as prescribed by a 2014 memorandum of understanding (MoU) on national security cases (Data Protection Act) between the Secretary of State for Justice and the Information Commissioner. The MoU provides guidelines for cooperation between the Information Commissioner's Office (ICO) and the security services.[103] The MoU relates to the ICO's enforcement powers under Sections 42 (Request for assessment) and 43 (Information notices) of the Act, with respect to instances in which the Section 28 exemption for national security cases is relied upon in response to subject access requests. The MoU circumscribes the extent and scope of information required to be provided by the security services in response to requests for information from the ICO. It explicitly endorses the Commissioner's power to assess whether the relevant exemptions justifying nondisclosure and/or the 'neither confirm nor deny response' have been properly relied on (powers under Part V of the DPA).[104] However, it sets out specific steps to be taken due to the sensitive nature of cases related to national security.[105] Specifically, the MoU emphasizes that cases should as much as possible be resolved "through dialogue and correspondence between the Commissioner and the relevant Department" and that, in the majority of cases, "a reasoned explanation together with any relevant background information […] will usually be sufficient to satisfy the Commissioner that the relevant exemptions have been properly relied on […] without disclosing to the Commissioner the detailed content of the withheld information or personal data […] .[106] In the exceptional cases that this reasoned explanation is not enough, the MoU recognizes that it might be necessary for the Commissioner to be granted confidential access to the withheld information or data, and the process and requirements to access these is set out in the MoU.[107] The MoU further states that the ICO's statutory enforcement powers (serving the security services with a formal information notice under Section 43 or enforcement notice under Section 40) should only be used if the case was not resolved through dialogue, and even in that case the MoU

[102] United Kingdom, HM Government (1998), *Data Protection Act 1998*, 16 July 1998, sch. 1, available at www.legislation.gov.uk/ukpga/1998/29.
[103] United Kingdom, Ministry of Justice (2014), 'Memorandum of understanding between on National Security Cases (FOIA and EIR)', January 2014, available at https://ico.org.uk/media/about-the-ico/documents/1042532/mou-national-security-cases-dpa.pdf.
[104] United Kingdom, Ministry of Justice (2014), 'Memorandum of understanding between on National Security Cases (FOIA and EIR)', January 2014, par. 6, available at https://ico.org.uk/media/about-the-ico/documents/1042532/mou-national-security-cases-dpa.pdf.
[105] United Kingdom, Ministry of Justice (2014), 'Memorandum of understanding between on National Security Cases (FOIA and EIR)', January 2014, par. 7, available at https://ico.org.uk/media/about-the-ico/documents/1042532/mou-national-security-cases-dpa.pdf.
[106] United Kingdom, Ministry of Justice (2014), 'Memorandum of understanding between on National Security Cases (FOIA and EIR)', January 2014, par. 11, available at https://ico.org.uk/media/about-the-ico/documents/1042532/mou-national-security-cases-dpa.pdf.
[107] United Kingdom, Ministry of Justice (2014), 'Memorandum of understanding between on National Security Cases (FOIA and EIR)', January 2014, par. 12, available at https://ico.org.uk/media/about-the-ico/documents/1042532/mou-national-security-cases-dpa.pdf.

stipulates that there should be further notification to the security services and consultation.[108] The consequences for the data subject's right to access the information or personal data are that the Commissioner cannot disclose either the reasoned explanation or the withheld information unless the relevant security services consent to the disclosure or all appeal proceedings have been exhausted.[109] Overall, in practical terms, the MoU seems to restrict the ICO's powers significantly and reduces the data subject's right to access to a mere right to request the Commissioner to verify the relevant security services' justifications for withholding information or personal data.

The case that led to the adoption of the MoU is *R. v. Information Tribunal*.[110] In this case, the Secretary of State had applied for judicial review of a decision of the National Security Appeals Panel allowing the appeal of the Information Commissioner under Section 28 (4) of the DPA against a certificate signed by the Secretary of State on the basis of Section 28 (2). In the case, an individual (X) had, on the basis of Section 7, applied to the Immigration and Nationality Directorate of the Home Department for information on any personal data held in respect of him. Dissatisfied with the response, X had requested the Information Commissioner to intervene. The Commissioner treated this as a "request for assessment" under Section 42 and wrote to the Home Department asking for disclosure of the withheld information. The Home Department replied that the national security exemption under Section 28 applied, that the nature of the disclosure given to X was in conformity with the government's policy with regard to matters involving security and intelligence agencies (namely, to "neither confirm or deny" the existence of information) and that the information would not be made available to the Commissioner. The Commissioner served a preliminary information notice on the Home Department followed by an information notice under Section 43. The Secretary of State subsequently signed a certificate under Section 28 (2) stating that an exemption was being claimed on the ground of national security, against which the Commissioner appealed to the tribunal. The Secretary argued that the Commissioner had no statutory powers that he could exercise under Part V of the DPA which could entitle him to second-guess a ministerial certificate. The tribunal held that, as both the Commissioner and the Secretary had roles to play within the context of Section 28 exemptions, the Commissioner's role could not be excluded on the ground of national security and that, as the Secretary had fundamentally misdirected himself as to the law, the certificate was liable to be quashed. Section 51 (1) entitled the Commissioner to check whether an exemption under Section 28 had been properly claimed.

The Investigatory Powers Bill will create an Investigatory Powers Commissioner who will be in charge of informing individuals about errors and their right to apply to the Investigatory Powers Tribunal.[111] According to Section 207, the Commissioner is obliged to inform individuals about "any relevant error" relating to them, only if a) the error is serious; and b) it is in the public interest for the individual to be informed about the error (Section 207 (1)). A relevant error is defined as an error "(a) by a public authority in complying with any requirements which are imposed on it by virtue of this Act or any other enactment and which are subject to review by a Judicial Commissioner, and (b) of a description identified for this purpose in a code of practice under Schedule 7" (Section 207 (9)). A serious error is defined

[108] United Kingdom, Ministry of Justice (2014), 'Memorandum of understanding between on National Security Cases (FOIA and EIR)', January 2014, paras. 13-14 and 25-29, available at https://ico.org.uk/media/about-the-ico/documents/1042532/mou-national-security-cases-dpa.pdf.

[109] United Kingdom, Ministry of Justice (2014), 'Memorandum of understanding between on National Security Cases (FOIA and EIR)', January 2014, par. 18, available at https://ico.org.uk/media/about-the-ico/documents/1042532/mou-national-security-cases-dpa.pdf.

[110] United Kingdom, Divisional Court, *R. (on the application of Secretary of State for the Home Department) v Information Tribunal*, [2006] EWHC 2958 (Admin), 23 November 2006. Case attached to final submission.

[111] United Kingdom, UK Parliament, *Investigatory Powers Bill*, 8 June 2016, s. 207, available at www.publications.parliament.uk/pa/bills/lbill/2016-2017/0040/17040.pdf

as an error which has caused "significant prejudice or harm to the person concerned" (Section 207 (2). The Commissioner must ask the public authority which has made the error to make submissions to him/her about the matters concerned prior to making a decision to inform (Section 207 (5)), and must consider the extent to which disclosing the error would be contrary to the public interest or prejudicial to (i) national security, (ii) the prevention or detection of serious crime, (iii) the economic well-being of the United Kingdom, or (iv) the continued discharge of the functions of any of the intelligence services (Section 207 (4)). In addition, the fact that there has been a breach of the ECHR is not considered by the Bill to be sufficient in itself for an error to be considered serious (Section 207 (3)).

3.2 Judicial remedies

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

The UK is not explicitly mentioned. It is not necessary to mention the UK for the relevance of FRA's analysis under this section.

3.2.1 Lack of specialisation and procedural obstacles

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

The UK is mentioned on page 67. The reference is correct. In addition, the Tribunal's Rules greatly restrict what information can be disclosed to a claimant in the course of their complaint. Rule 6 (2) provides that the Tribunal can withhold any information or document disclosed or provided during proceedings, and does not need to disclose to the claimant the fact that an oral hearing has taken place. The Tribunal is, in any event, under no obligation to hold oral hearings (Rule 9 (2)). Complainants will be notified of the outcome of the case. If a determination is made in favour of the complainant the findings of fact must be provided. Complainants are not however entitled to be informed of the reasons of decisions not made in their favour (Rule 13).

3.2.2 Specialised judges and quasi-judicial tribunals

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

The UK is mentioned on pages 68-69. The Investigatory Powers Bill will create the possibility to appeal the Investigatory Powers Tribunal's decisions.[112] In addition, on 22 June

[112] United Kingdom, UK Parliament, *Investigatory Powers Bill*, 8 June 2016, s. 217, available at www.publications.parliament.uk/pa/bills/lbill/2016-2017/0040/17040.pdf

2015, the Tribunal, following on from *Liberty & Others* mentioned in the first paragraph on page 69 and further, made determinations in favour of Amnesty International and the Legal Resources Centre, providing some factual basis for the findings in each.[113]

3.3 Non-judicial remedies: independence, mandate and powers

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

The UK is not explicitly mentioned. It is not necessary to mention the UK for the relevance of FRA's analysis under this section.

3.3.1 Types of non-judicial bodies

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

The UK is mentioned on page 70. The reference is correct.

3.3.2 The issue of independence

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

The UK is not explicitly mentioned. It is not necessary to mention the UK for the relevance of FRA's analysis under this section.

3.3.3 Powers and specialisation of non-judicial remedial bodies

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

The UK is not explicitly mentioned. It is not necessary to mention the UK for the relevance of FRA's analysis under this section.

FRA key findings

[113] United Kingdom, Investigatory Powers Tribunal, UKIPTrib 13_77-H 2, 22 June 2015, pars. 14 and 15, available at www.ipt-uk.com/docs/Final_Liberty_Ors_Open_Determination_Amended.pdf.

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

The UK is not explicitly mentioned. It is not necessary to mention the UK for the relevance of FRA's analysis under this section.

Conclusions

1. *If your Member State is mentioned in this chapter/section/sub-section, please check the accuracy of the reference.*
2. *If you Member State is mentioned, please update the data (new legislation, new report etc.)*
3. *If you Member State is not mentioned, please provide data that would call for a specific reference given the relevance of the situation in your Member State to illustrate/complement FRA comparative analysis.*

The UK is not explicitly mentioned. It is not necessary to mention the UK for the relevance of FRA's analysis under this section.

1.5 Check the accuracy of the figures and tables published in the FRA report (see the annex on Figures and Tables)

1.5.1 Overview of security and intelligence services in the EU-28

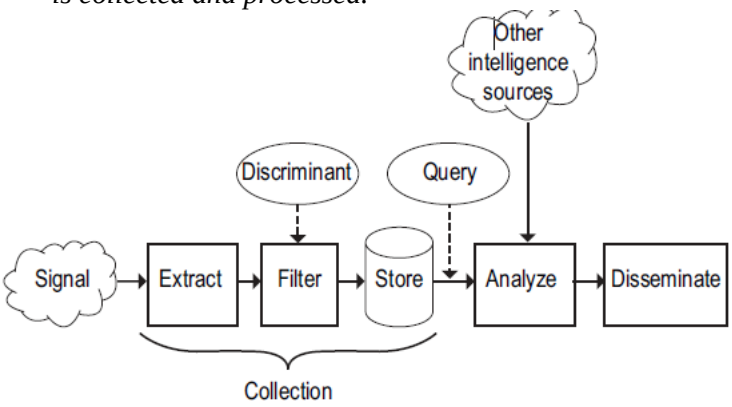
- *Please, delete all lines not referring to your country in the table below (see Annex p. 93 of the FRA Report)*
- *Check accuracy of the data*
- *Add in track changes any missing information (incl. translation and abbreviation in the original language).*
- *Provide the reference to the national legal framework when updating the table.*

	Civil (internal)	Civil (external)	Civil (internal and external)	Military
UK	British Security Service (BSS) or MI5	Secret Intelligence Service (SIS) or MI6 Government Communications Headquarters (GCHQ)		Defence Intelligence (DI)

The table is correct.

1.5.2 Figure 1: A conceptual model of signals intelligence

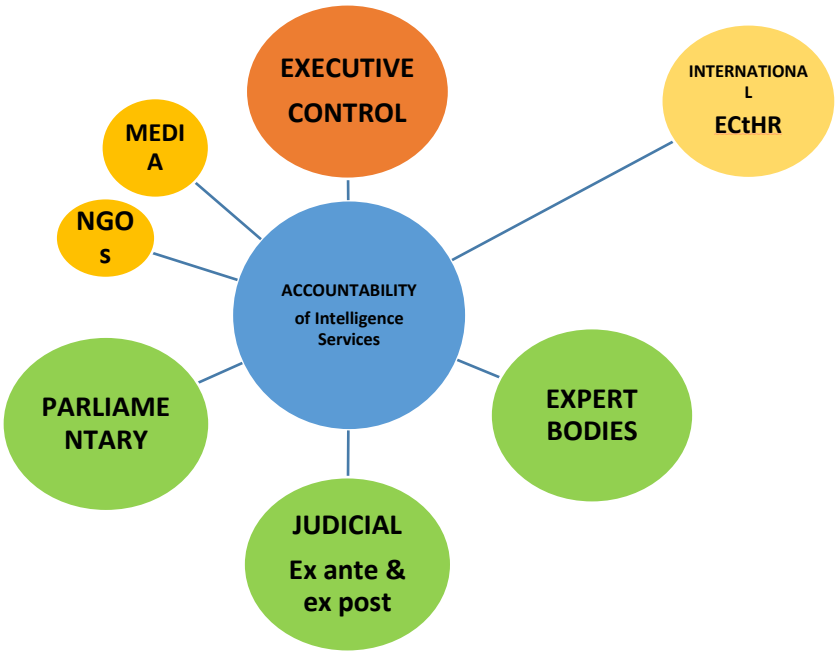
- *Please, provide a reference to any alternative figure to Figure 1 below (p. 16 of the FRA Report) available in your Member State describing the way signals intelligence is collected and processed.*



No alternative figure describing the way signals intelligence is collected and processed is available in the UK.

1.5.3 Figure 2: Intelligence services' accountability mechanisms

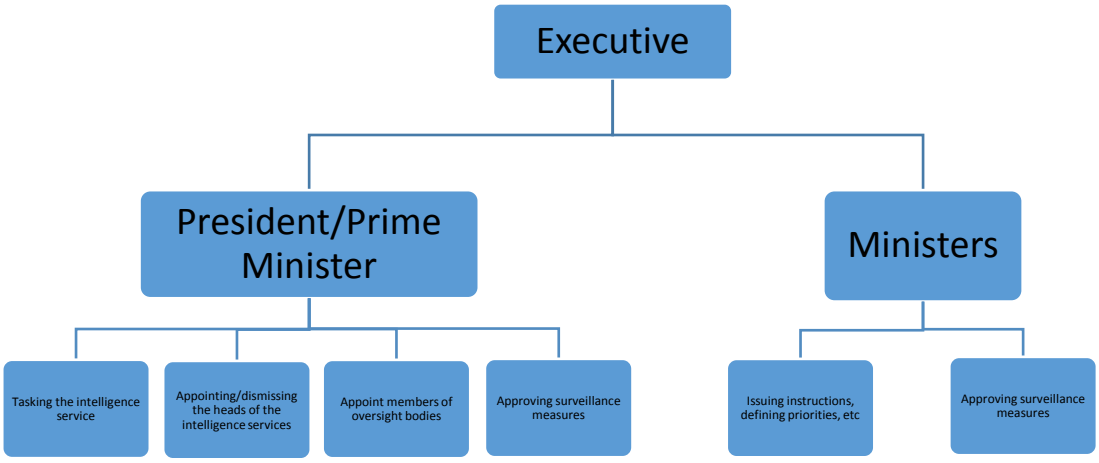
Please confirm that Figure 2 below (p. 31 of the FRA Report) illustrates the situation in your Member State in an accurate manner. If it is not the case, please suggest any amendment(s) as appropriate and substantiate it/them with specific reference to the legal framework.



This figure illustrates the situation in the UK in an accurate manner. However, *ex ante* judicial control is currently not yet possible but this will be introduced by the Investigatory Powers Bill, in its current form in Sections 21, 97, 123, 139, 157 and 179.

1.5.4 Figure 3: Forms of control over the intelligence services by the executive across the EU-28

Please confirm that Figure 3 below (p. 33 of the FRA Report) properly captures the executive control over the intelligence services in your Member State. If it is not the case, please suggest any amendment(s) as appropriate and substantiate it/them with specific reference to the legal framework.



This figure properly captures the executive control over the intelligence services in the UK.

1.5.5 Table 1: Categories of powers exercised by the parliamentary committees as established by law

Please, delete all lines not referring to your country in the table below (see p. 36 of the FRA Report)
Please check the accuracy of the data. Please confirm that the parliamentary committee in your Member State was properly categorised by enumerating the powers it has as listed on p. 35 of the FRA Report. Please suggest any amendment(s) as appropriate and substantiate it/them with specific reference to the legal framework.

Member States	Essential powers	Enhanced powers
UK	X	

Note: Finland, Ireland, Malta and Portugal do not have parliamentary committees that deal with intelligence services.

This table is correct.

1.5.6 Table 2: Expert bodies in charge of overseeing surveillance, EU-28

Please, delete all lines not referring to your country in the table below (p. 42 of the FRA Report). Please check the accuracy of the data. In case of inaccuracy, please suggest any amendment(s) as appropriate and substantiate it/them with specific reference to the legal framework.

EU Member State	Expert Bodies
UK	Intelligence Services Commissioner Interception of Communications Commissioner Investigatory Powers Tribunal

This table is correct. If the Investigatory Powers Bill is accepted in its current form, the Intelligence Services Commissioner and the Interception of Communications Commissioner will be replaced by the Investigatory Powers Commissioner (Section 215 of the Bill).

1.5.7 Table 3: DPAs' powers over national intelligence services, EU-28

Please, delete all lines not referring to your country in the table below (p. 49 of the FRA Report). Please check the accuracy of the data. In case of inaccuracy, please suggest any amendment(s) as appropriate and substantiate it/them with specific reference to the legal framework.

EU Member State	No powers	Same powers (as over other data controllers)	Limited powers
UK			X

Notes: *No powers: refers to DPAs that have no competence to supervise NIS.*

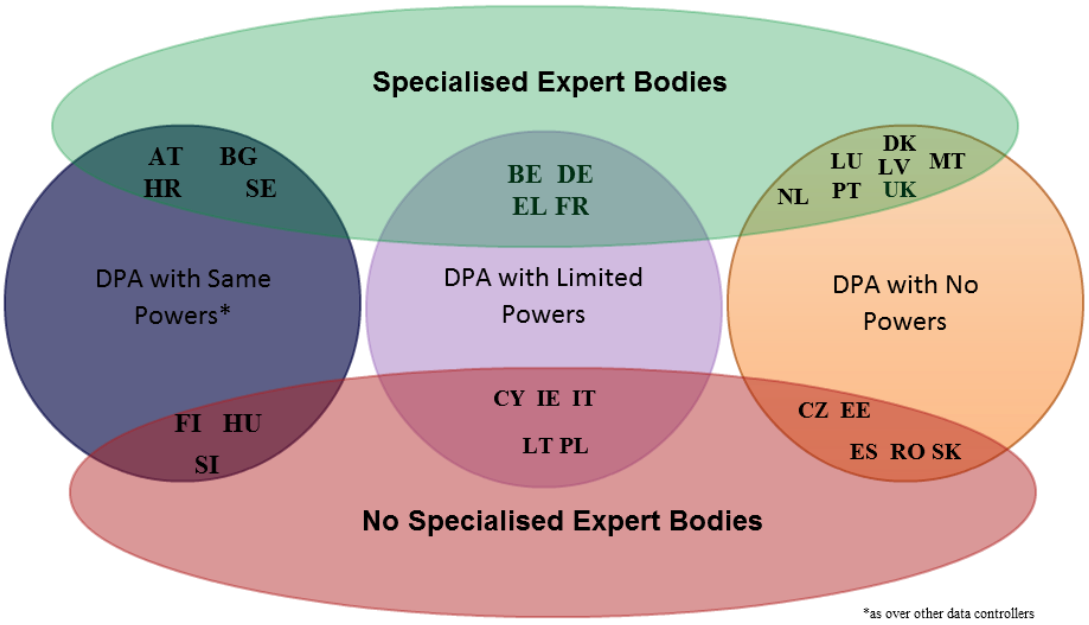
Same powers: refers to DPAs that have the exact same powers over NIS as over any other data controller.

Limited powers: refers to a reduced set of powers (usually comprising investigatory, advisory, intervention and sanctioning powers) or to additional formal requirements for exercising them.

This table is correct. If the Investigatory Powers Bill is accepted in its current form, the UK's DPA (the Information Commissioner) will be given some powers, namely to "audit compliance with requirements or restrictions imposed by virtue of Part 4 [retention of communications data] in relation to the integrity, security or destruction of data retained by virtue of that Part" (Section 219 of the Bill). It will be possible to retain data on the basis of national security (Section 83 (1) c.f. Section 58 (7) (a)) but the ICO's specific powers in relation to this are not yet clear at this stage of the legislative process.

1.5.8 Figure 4: Specialised expert bodies and DPAs across the EU-28

Please check the accuracy of Figure 4 below (p. 50 of the FRA Report). In case of inaccuracy, please suggest any amendment(s) as appropriate and substantiate it/them with specific reference to the legal framework.



This table is correct. However, if the Investigatory Powers Bill is accepted in its current form, the UK should be moved to Specialised Expert Bodies/DPA with Limited Powers (see above).

1.5.9 Table 4: Prior approval of targeted surveillance measures, EU-28

Please, delete all lines not referring to your country in the table below (p. 52 of the FRA Report). Please check the accuracy of the data. In case of inaccuracy, please suggest any amendment(s) as appropriate and substantiate it/them with specific reference to the legal framework.

EU Member State	Judicial	Parliamentary	Executive	Expert bodies	None
UK			X		

This table is correct. However, if the Investigatory Powers Bill is accepted in its current form, the "Judicial" box should be ticked too (Sections 23 and 102 of the Bill).

1.5.10 Table 5: Approval of signals intelligence in France, Germany, the Netherlands, Sweden and the United Kingdom

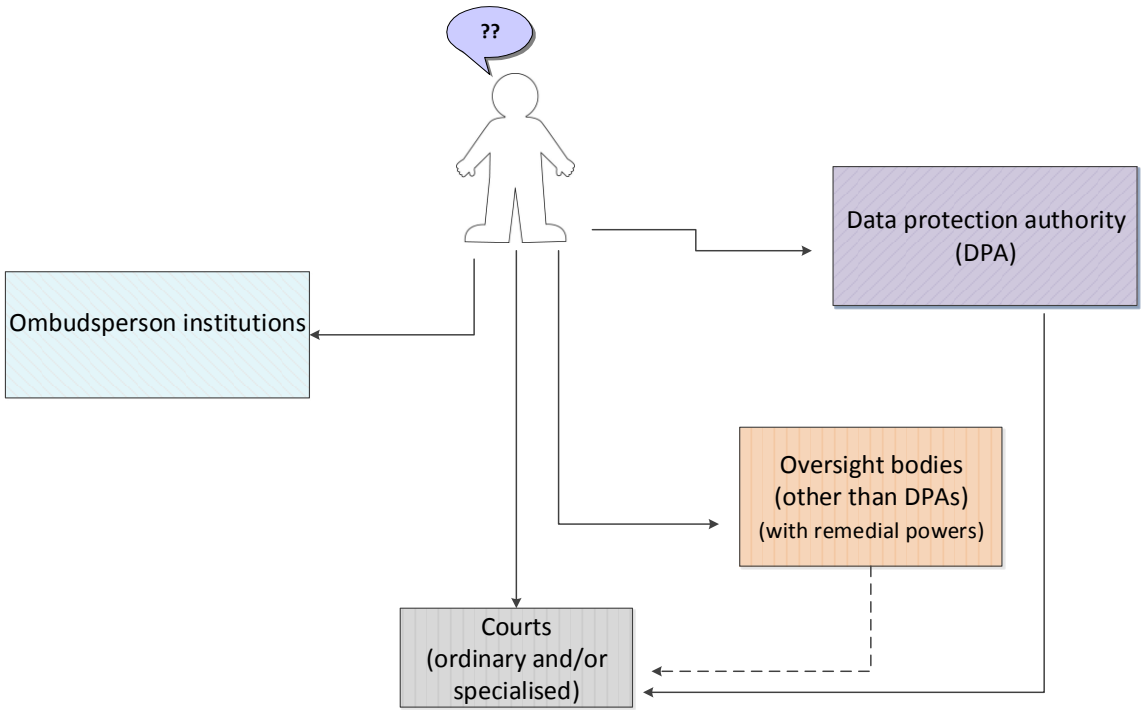
Please check the accuracy of Table 5 below (p. 55 of the FRA Report). In case of inaccuracy, please suggest any amendment(s) as appropriate and substantiate it/them with specific reference to the legal framework.

EU Member State	Judicial	Parliamentary	Executive	Expert
UK			X	

This table is correct. However, if the Investigatory Powers Bill is accepted in its current form, the "Judicial" box should be ticked too (Sections 131, 147, 165 and 188 of the Bill).

1.5.11 Figure 5: Remedial avenues at the national level

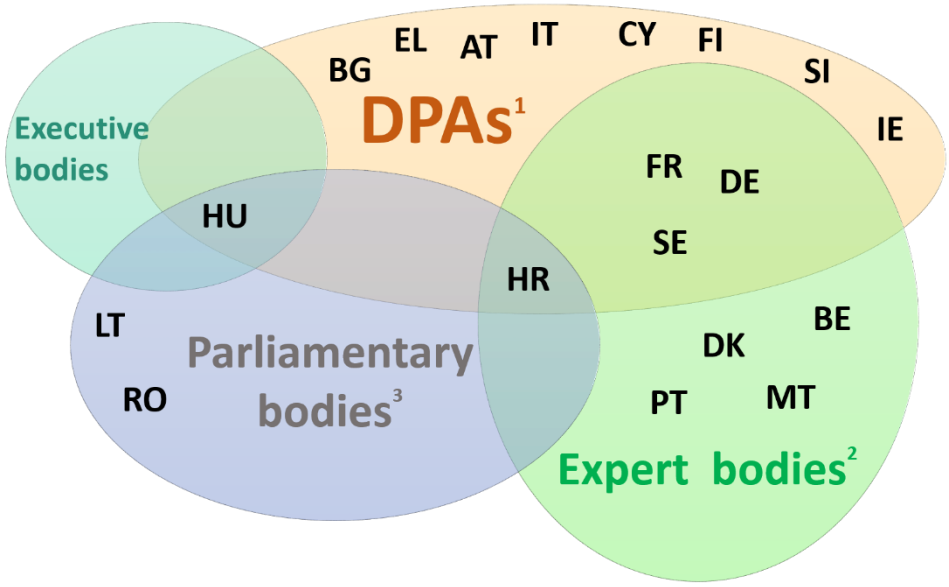
Please confirm that Figure 5 below (p. 60 of the FRA Report) illustrates the situation in your Member State in an accurate manner. If it is not the case, please suggest any amendment(s) as appropriate and substantiate it/them with specific reference to the legal framework.



In the UK, the only remedial avenue available is the Investigatory Powers Tribunal. Additionally, if the Investigatory Powers Bill is accepted in its current form, an Investigatory Powers Commissioner will be created who will be in charge of informing individuals about errors and their right to apply to the Investigatory Powers Tribunal (Section 207).

1.5.12 Figure 6: Types of national oversight bodies with powers to hear individual complaints in the context of surveillance, by EU Member States

Please check the accuracy of Figure 6 (p. 73 of the FRA Report) below. In case of inaccuracy, please suggest any amendment(s) as appropriate and substantiate it/them with specific reference to the legal framework.



Notes: 1. The following should be noted regarding national data protection authorities: In Germany, the DPA may issue binding decisions only in cases that do not fall within the competence of the G 10 Commission. As for 'open-sky data', its competence in general, including its remedial power, is the subject of on-going discussions, including those of the NSA Committee of Inquiry of the German Federal Parliament

2. *The following should be noted regarding national expert oversight bodies: In Croatia and Portugal, the expert bodies have the power to review individual complaints, but do not issue binding decisions. In France, the National Commission of Control of the Intelligence Techniques (CNCTR) also only adopts non-binding opinions. However, the CNCTR can bring the case to the Council of State upon a refusal to follow its opinion. In Belgium, there are two expert bodies, but only Standing Committee I can review individual complaints and issue non-binding decisions. In Malta, the Commissioner for the Security Services is appointed by, and accountable only to, the prime minister. Its decisions cannot be appealed. In Sweden, seven members of the Swedish Defence Intelligence Commission are appointed by the government, and its chair and vice chair must be or have been judges. The remaining members are nominated by parliament.*

3. *The following should be noted regarding national parliamentary oversight bodies: only the decisions of the parliamentary body in Romania are of a binding nature.*

This figure is correct.