FRA

Thematic Legal Study on assessment of data protection measures and relevant institutions [United Kingdom]

Douwe Korff
[Nottingham][UK]
February 2009

Contents

Executive summary

Overview

[1]. The UK Information Commissioner warned in 2004 that Britain was 'sleepwalking into a surveillance society', and added in 2006 that it had actually already woken up in one.

[2]. Part of the explanation is that data protection in the UK has a weaker constitutional basis than in most - possibly all - other EU Member States. The *Data Protection Act 1998* (DPA98) would appear to fall short of Directive 95/46/EC in many respects; and the Government is proposing to allow data sharing on terms that are likely to violate European law. Even so, the UK data protection authority, the *Information Commissioner's Office* (ICO), does not feel called upon to address the issue of EC law- or ECHR compliance. Enforcement of the DPA98 (and a fortiori of European law and -principles) is also weak. In addition, the courts in the country are disinclined to give strong protection to personal information and privacy. These factors combine to create a data protection regime in the UK that is notably less-developed, and weaker, and less enforced, than the data protection regimes in other EU Member States.

[3]. The *Data Protection Act 1998* (DPA98), adopted in order to implement Directive 95/46/EC, came into force on 1 March 2000, together with a large number of Statutory Instruments, which provide additional detailed regulation. The UK has since adopted the *Privacy and Electronic Communications (EC Directive) Regulations 2003* (PERC) and the *Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2004*, to implement Directive 2002/58/EC.

[4]. Directive 2006/24/EC on the retention of telecommunications data has not (yet) been implemented by means of a law. Instead, the UK is relying on a Code of Practice on Data Retention approved by Parliament in December 2003 in the form of the *Retention of Communications Data (Code of Practice) Order 2003* (but which does not have force of law), and on certain informal, supposedly voluntary measures adopted by a number of the UK's Internet Service Providers (ISP), under which the latter retain the relevant data.

[5]. In fact, many matters - also under the DPA98 and PERC - are addressed not in formally binding rules or regulations, but in non-binding 'legal guidance', 'codes of practice', 'guidance notes', 'good practices notes', 'technical guidance notes', and simpler leaflets directed at the general public issued by the ICO and the Ministry of Justice. This adds to the overall weakness of the regime.

Data Protection Authority

[6]. **General:** In 2001, the UK data protection supervisory authority was renamed the Information Commissioner after it was also, separately, charged with supervision over the UK *Freedom of Information Act 2000* (FOIA). In practice, and on its own website, the authority is referred to as the *Information Commissioner's Office* or ICO. It has some 260+ staff and will have a budget of +£16 million in the coming year. The ICO operates under a *Framework Document* comprising a *Management Statement* and a *Financial Memorandum*, concluded between it and its 'sponsoring' Government office, currently the Ministry of Justice.

[7]. The above means that the ICO is quite tightly controlled by the Government. It is therefore doubtful whether the office can be said to fulfil the requirements set out in Article 28(1) of the Directive, which stipulates that Member States must establish national supervisory authorities of such a kind that it is ensured that they 'shall act with complete independence in exercising the functions entrusted to them.'

[8]. **Powers and duties of the DPA:** A major responsibility of the ICO is to receive notifications from data controllers and maintain a register of all such controllers. The ICO is entirely dependent on the fees from notification for its data protection work. There are some 287,000 registered controllers.

[9]. Contrary to Article 28(2) of Directive 95/46/EC, the ICO is not required to be consulted by central or other bodies when those bodies draw up 'administrative measures or regulations relating to the protection of individuals' rights and freedoms with regard to the processing of personal data.'

[10]. Different from many other Member States, in the UK the ICO does not have any autonomous powers of access to data, or premises, on demand, of his own motion; instead, he must apply for a search warrant from a judge. In 2006-07, seven warrants were applied for (and presumably granted).

[11]. The Information Commissioner can carry out an audit of a controller's operations, but only at the latter's request. In the year 2006-07, the ICO carried out eight audits of processing operations of public bodies, at the request of those authorities. There are proposals to give the ICO power to demand an audit of public bodies (but he would like to also have that power in respect of private entities).

[12]. The Commissioner can already issue so-called 'Information-' and 'Enforcement Notices' of his own motion. The former is a notice requiring an organisation or person to supply the Commissioner with specified information; the latter is an order requiring a controller to do (or not to do) certain things. Both are sparingly used (see below: Enforcement in practice).

[13]. Recipients of such notices can appeal to a special appellate body, the *Information Tribunal*, if they disagree with the (terms of the) notice. Since the coming into force of the DPA98, there have been only nine cases decided by the Tribunal in which reference was made to that Act; only three primarily concerned the DPA98. Controllers can appeal from a ruling of the Tribunal to the High Court, but this has only happened once in respect of the DPA98. Data subjects do not have a right to bring cases affecting them to the Tribunal.

[14]. Under the DPA98, the Secretary of State can specify that certain 'risky' operations will be subject to a 'prior assessment' (what the Directive calls a 'prior check'), but in practice this has never been done.

[15]. The DPA98 sets out a number of criminal offences. Most of them relate to notification or supervision or enforcement measures. The ICO invokes these provisions also most sparingly: there were 14 prosecutions in 2006-07.

[16]. The Information Commissioner must submit annually to Parliament 'a general report on the exercise of his functions under this Act.' He may also submit to it 'such other reports with respect to those functions as he thinks fit'; and he must also submit any sectoral code of practice to Parliament, when it is a code that the Secretary of State has ordered to be drawn up. However, these provisions are not really used in the manner suggested by Article 28(3) of the Directive, which speaks of the national supervisory authority 'referring [a specific] matter to national parliaments or other political Institutions'.

[17]. **Enforcement in practice:** The ICO does not go out of his way to try and uncover breaches of the Act unless they somehow become exposed, usually because of a complaint or a series of complaints. In the last reporting year, he received some 24,000 cases. There must be many more violations of the law, in particular of the duty to notify (register). Specifically, only a small fraction of the 2.3 million registered companies notify, although it would appear that most - perhaps 1.5 million - should. Yet companies that don't even bother to notify their operations are presumably also unlikely to take their more onerous data protection duties seriously.

[18]. Even in the cases that are brought to the ICO's attention, enforcement is not forceful. Of the 24,000 submitted in 2006-07:

- most cases (13,400) were dealt with 'simply' through 'advice and guidance' (even though some of these cases were 'extremely complex'), without an assessment of whether the law was breached;
- more than a third of the remaining 10,000+ cases were also not assessed with a view to determining whether the law had been broken because they did not meet the ICO's 'assessment criteria'; and
- the ICO found that it was 'likely' that a breach of the law had occurred in 3,600 of the remaining 6,500 or so cases.

[19]. Yet even the latter category is not very forcibly pursued. Specifically, the ICO rarely resorts to the issuing of Information- or Enforcement Notices. The Commissioner and his staff prefer to first raise the issue with any person or organisation concerned, and attempt to resolve the matter 'by negotiation or other less formal means'. Such 'negotiated resolutions' can be backed by a formal undertaking given by an organisation to the Commissioner. Overall, six Enforcement Notices were issued in the year 2006-07; the ICO has obtained some 36 formal undertakings over several years. Some of these related to 'hundreds' of complaints. Even so, they can represent only a fraction of the 3,600 cases of 'likely' violations of the law. Presumably, all the cases (of this total) that did not involve undertakings, enforcement notices or prosecutions were resolved in other ways (typically, by negotiation), to the satisfaction of the ICO.

[20]. The ICO's approach may give the impression of 'soft' and negotiable enforcement of the law, which is not conducive to wider compliance and may in part account for the widespread disregard for even the most basic requirement of the Act, notification of processing operations. This problem is not unique to the UK - similar criticism is voiced in other EU Member States. But it contributes to the overall weakness of data protection in the UK legal order, already encouraged by the weak constitutional/legal basis it has in the country (as noted above).

[21]. The 'negotiable' approach to data protection, adopted by the ICO, also means that justice is not seen to be done - which is contrary to the Rule of Law, and feeds suspicions that big companies and organisations can negotiate arrangements that are not in accordance with the Act as others than the ICO would read it - or with the Directive or the ECHR, which the ICO doesn't take into account in any case. What is more, it means that the law is not openly developed, in a way that allows for public debate and criticism. This is not healthy.

Compliance

[22]. As already noted, compliance with the DPA98 is not very high, if one judges this by the number of registered controllers, which is only a fraction of the number one would expect if there were to be full compliance (less than 300,000 registered controllers in the UK overall, in contrast to some 2.300,000 registered companies in Great Britain alone, without counting individuals that may need to register, or public-sector bodies).

[23]. The cases that are pursued through enforcement action (notices, undertakings and prosecutions) tend to revolve around easy-to-notice matters such as failure to notify, unsolicited telemarketing, persistent criminal obtaining and selling of information, or blatant security failures. More intricate matters are (as far as can

be gleaned from the ICO's reports) not the subject of enforcement action. With enforcement being 'soft' and focussing on such 'low-hanging fruit', it must be assumed that compliance in other areas is also low.

[24]. Some serious, high-profile matters, over which deep concern is expressed at the European level - such as the SWIFT (banking) and PNR (airline passenger data) issues, and the question of collecting and retaining by the police of DNA samples from arrested persons - are only half-heartedly pursued, if at all.

Sanctions, Compensation and Legal Consequences

[25]. As already noted, enforcement of data protection in the UK is 'soft': most cases are not even assessed with a view to determining if the law was breached; Information- and Enforcement Notices are very sparingly used even in cases in which it is found that a breach of the law was 'likely'; and prosecutions are initiated in only a minute fraction of all cases in which there was a criminal breach of the Act. Rather, most cases that are assessed end in a 'negotiated resolution'. There is little insight into the terms on which these negotiations are settled - which raises serious doubts about both the acceptability of such settlements and the specific application of the law (and the Directives) in the UK.

[26]. Individual complainants have no effective possibility to challenge the outcome of such negotiations, even in cases that affect them. In particular, unlike controllers, individual complainants cannot appeal to the *Information Tribunal*. They can, in theory, apply for judicial review of the ICO's decisions and actions, but that is a costly and time-consuming remedy, with uncertain outcome and of limited scope.

[27]. The only way in which individuals can assert their rights is by taking their case to court: they can claim actual damages for breaches of the law that affected them, but can only seek compensation for distress (immaterial damages) in cases in which they have first shown that they suffered actual (material) loss. They can also ask the court to order a defendant to act, or cease to act, in a particular way, to comply with the DPA98.

[28]. Overall, the status of people who claim to be victims of violations of the DPA98 is therefore weak, and not much strengthened by the ICO. The Office will help individuals who it deems to have a meritorious case (especially if there are many of them and there is evidence of a widespread problem), and it will seek on their behalf an 'acceptable' solution to their problems, based on its (the ICO's) views of what strikes a reasonable balance between the interests of the complainants and those of the controllers. But it will not give much support to

individuals who seek a strict, uncompromising application of the law, or who disagree with the ICO on a particular interpretation of a particular term in the Act (or who argue that an issue arises in relation to one of the EC directives or the ECHR).

Rights Awareness

[29]. The ICO publishes many guides and leaflets on the application of the DPA98, hosts an extensive website, and generates extensive publicity. As a result, there is now clearly widespread awareness amongst the public and data managing professionals of the existence of the DPA98 and data protection generally, and of specific rights and duties under the Act. 82 % of individuals are aware of their rights, and 94% of practitioners are aware of the requirements of the law.

Analysis of deficiencies

[30]. The deficiencies in the UK regime have already been noted. Briefly:

- data protection has a weak constitutional basis;
- the courts are disinclined to give strong protection to personal information and privacy;
- the DPA98 fails to properly implement Directive 95/46/EC, and many matters are regulated not through binding law but by means of non-binding guidance;
- the UK Data Protection Authority (DPA), the ICO, is quite tightly controlled by Government; it is doubtful whether the ICO has a sufficiently independent status in terms of the Directive;
- the ICO does not apply EC law or ECHR principles in his enforcement of the DPA98;
- its enforcement of the DPA98 is generally 'soft' and aimed at reaching 'negotiated resolutions' to issues, rather than at strict application of the law; tougher enforcement measures such as the imposition of Enforcement Notices or prosecutions are reserved for a very few, easy-to-prove cases of manifest abuse;
- the details of the 'negotiated resolutions' reached in the vast majority of cases are not made public and the application of the law is therefore not transparent;
- it is difficult for individuals to assert their rights: the ICO provides only limited support to them (again, aimed mainly at reaching 'negotiated

resolutions', without involving the individuals in the negotiations); for 'harder' enforcement, or to obtain compensation, they must go to court, which is expensive and time-consuming;

- compliance with the law is (unsurprisingly) very low; some major issues 'flagged' at the European level (SWIFT, PNR, DNA) are hardly pursued.

Good Practice

[31]. The ICO does good work in terms of issuing guides and leaflets etc. (even if not everyone will always agree with all he says), and raising data protection awareness generally.

[32]. The ICO is also undoubtedly regarded as an important advisor to public and private bodies, and will claim to have had a significant impact on Government- and private-sector policies and practices (although again, the Commissioner has been criticised for sometimes accepting or seeming to endorse dubious practices).

Miscellaneous

[33]. The issues in the UK are complex, both in law and in practice. This report can only provide a basic insight into them. It should also be stressed that some (perhaps many) of the critical remarks made in this report could equally be made in respect of other countries, and other DPAs - but the authors of those other reports may have approached their task differently, less critical. Care should therefore be taken in drawing comparative conclusions too easily or quickly from this report.

1. Overview

1.1. Constitutional and International Standards

[34]. The United Kingdom (UK) does not have a written constitution or a Bill of Rights, setting out the rights of the individuals, and the way in which they can be limited, in a comprehensive manner.[1] There is therefore no supra-statutory right or principle on which data protection can be based (as is the case in, say, Germany, Italy or Spain). The related concepts of privacy and confidentiality remain ill-defined in law (especially common law). Data protection is therefore effectively still mainly built on a simple statutory and regulatory basis (with much additional 'guidance' indeed issued in non-binding form, as further described at 1.2, below).

[35]. The UK is a party to the *European Convention on Human Rights* (ECHR) and to the Council of Europe *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.*[2] It has signed but not yet ratified the Additional Protocol to the latter Convention,[3] and it has neither signed nor ratified the *Convention on Human Rights and Biomedicine.*[4]

[36]. Under the traditional UK 'dualist' legal doctrine, international treaties - even international treaties that have been ratified by the UK - do not have any direct internal effect in the UK legal order; they cannot, as such, be invoked or relied on in English courts. However, since 2000, the *European Convention on Human Rights* **is** incorporated into UK law, through the *Human Rights Act 1998*[5] (HRA). Article 8 of the Convention is part of the basis of European data protection law, and increasingly interpreted as comprising data protection

1 The drafting of 'a "British Bill of Rights" of some kind' is currently under consideration. See: L Maer, A.Horne 2008) *Background to proposals for a British Bill of Rights and Duties* House of Commons Library, available at: http://www.parliament.uk/commons/lib/research/briefings/snpc-04559.pdf (20.01.2009).

2 Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, CETS No.: 108, 01.10.1985.

3 Council of Europe, Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows, CETS No.: 181, 01.07.2004.

4 Council of Europe, Convention for the protection of Human Rights and dignity of the human being with regard to the application of biology and medicine: Convention on Human Rights and Biomedicine, CETS No.: 164, 01.12.1999.

5 UK/ Human Rights Act 1998 c.42 (09.11.1998), available at: http://www.opsi.gov.uk/ACTS/acts1998/ukpga_19980042_en_1#pb3-l1g6 (23.01.2009).

principles.[6] Under the HRA, the substantive provisions of the ECHR, including Article 8, are binding on all public bodies - including the *Information Commissioners Office* (ICO) as the watchdog over any such data sharing. Any acts by any such bodies which are claimed to breach Article 8 can be challenged in the British courts, and will be struck down if they are held to have done so.

[37]. In principle, even the legislator is required to abide by the requirements of the Convention as reflected in the HRA, even if, for historical/constitutional reasons, the judiciary cannot declare an Act of Parliament invalid: the courts may in cases in which an Act of Parliament fails to comply with the Convention/the HRA, instead issue a 'declaration of incompatibility', and it is then up to the Government to initiate remedial legislative action. This does give human rights generally, and data protection insofar as governed by Article 8 ECHR, an at least somewhat enhanced status.

[38]. The UK is of course also a Member of the European Union and, as such, required to properly and fully implement EC directives, including the data protection directives, 95/46/EC, 2002/58/EC and 2006/24/EC. Under the *European Communities Act 1972*,[7] European Community law overrides UK law (statutory or common law) (see s.2 of the Act).

[39]. However, there are few, if any, cases in which European data protection principles have been applied by the UK courts to reinforce data protection in the UK beyond the basic (indeed, insufficient) requirements of the *1998 Data Protection Act*[8] (DPA98) (see the next paragraph). In the few data protection cases that have reached the higher UK courts - and in particular in the *Durant*[9] case, further discussed in section 2.2.4, below, the UK courts have, if anything, applied data protection concepts and principles at a level below the European minimum standards.

[40]. An additional problem is that the UK DPA98 in many ways fails to fully implement the requirements of the main EC data protection directive. It has been reported that the European Commission is investigating alleged failings by the UK to properly implement eleven of the Directive's thirty-four articles,

---

6 Cf. the references to privacy and Article 8 ECHR in the Explanatory Memorandum to Council of Europe Convention No. 108 and in the 10th Preamble to Directive 95/46/EC. For an analysis of some of the leading ECHR (and ECJ) cases in this respect (up to end-2003), see D. Korff (2004) 'The legal framework - an analysis of the "constitutional" European approach to issues of data protection and law enforcement', in: I. Brown & D. Korff (2004) *Privacy & Law Enforcement*, study for the UK Information Commissioner. The trend to recognise data protection as part of the protection accorded under Article 8 ECHR has if anything been reinforced in subsequent judgments of the Strasbourg Court.

7 UK/European Communities Act c.68 (17.10.1972), available at: http://www.opsi.gov.uk/Acts/acts1972/ukpga_19720068_en_1 (26.01.2009).

8 UK/Data Protection Act c.29 (16.07.1998), available at: http://www.opsi.gov.uk/Acts/Acts1998/ukpga_19980029_en_1 (26.01.2009).

9 *Durant v Financial Services Authority* [2003] EWCA Civ 1746.

almost a third of the entire directive.[10] Although the UK Government still claims that it has implemented the Directive fully, many deficiencies have been pointed out by activists and academics (including the author of the present report).[11]

[41]. Even more problematic, the *Information Commissioner's Office* (ICO) has made it clear that it feels that it is not its task to ensure that the UK DPA98 is applied in a way consistent with the EC Directives, or to point out where the Act might fail to meet the requirements of the Directive. The ICO applies only the DPA98, as it appears on its face.[12]

[42]. At the same time, the Government's so-called 'Transformational Government' policy is leading to ever-increasing data collection and –sharing. The latest development is a proposal which could result in the effective abolishing of data protection restrictions on the sharing of data within the public sector.[13]

---

10 'Europe claims UK botched one third of Data Protection Directive', *Out-Law News*, 17 September 2007, available at: http://www.out-law.com/page-8472 (26.01.2009). Although this is, as such, a media article, it is based on information obtained directly from the authorities concerned under freedom of information law, and both the UK Government and the Commission confirmed that various issues were being discussed, without being specific. However, the information obtained by Out-Law showed that "the articles of the Directive which the Commission claims have not been implemented properly are articles 2, 3, 8, 10, 11, 12, 13, 22, 23, 25 and 28 ... These Articles relate to: the definitions used in the Directive (e.g. the meaning of personal data); the scope of the Directive's application to manual files; the conditions when sensitive personal data can be processed; the fair processing notices give to individuals; the rights granted to data subjects; the application of exemptions from these rights; the ability of individuals to seek a remedy when there is a breach; the liability of organisations for breaches of data protection law; the transfer of personal data outside European Union; and the powers of the Information Commissioner.'

11 E.g., D. Korff (2008) 'UK Data Sharing: European Conflict', in: *Data Protection Law & Policy*, p.12ff. Other issues were raised in the enquiry mentioned in the next footnote, and in R. Thomas and M. Walport (2008) *Data Sharing Review Report*, available at: http://www.justice.gov.uk/docs/data-sharing-review-report.pdf (26.01.2009).

12 As it was put by the Assistant Information Commissioner, Jonathan Bamford, in answer to a question by a House of Commons Select Committee during hearings on the Electronic Patient Record being introduced in the National Health Service, in a session in May 2007 in which the author of the current report had mentioned the alleged failures of the UK Act to comply with the Directive: 'If there is any issue to do with whether the UK Data Protection Act correctly implements the EU Data Protection Directive that is a matter for the Ministry of Justice, as it is now, because that is the body which is responsible for ensuring that we implement the Directive in UK law. If there is a concern about a difference it is for the Ministry of Justice to answer that point. The Information Commissioner is charged with implementing the UK Data Protection Act...If you have a real concern [about any failure of the Act to properly implement the Directive], I believe it is important that you speak to the Ministry of Justice as part of this inquiry.' Answer to Question 176 at the Select Committee hearing on 10 May 2007. Full transcript available at: http://www.parliament.the-stationery-office.co.uk/pa/cm200607/cmselect/cmhealth/422/7051002.htm (26.01.2009).

13 The proposals are contained in the *Coroners and Justice Bill*, which is currently before Parliament. The data sharing would be based on ministerial orders. The law, if adopted, would require ministers who want to issue such an order to hold a formal consultation and obtain a report from the Information Commissioner, and the order would need parliamentary approval

[43]. Mention should finally be made of the fact that the House of Lords Constitution Committee has launched a wide inquiry into the impact that government surveillance and data collection have upon the privacy of citizens and their relationship with the State. As the Committee's webpage explains: 'The inquiry, which is set against a backdrop of increased use of CCTV, the creation of the national DNA database, the new NHS Spine and the proposals for ID cards, will seek to find out if increased surveillance and data collection by the state have fundamentally altered the way it relates to its citizens.'[14] Launched in 2007, the inquiry is expected to issue its report in the spring of 2009.

[44]. In sum: Data protection in the UK has a weaker constitutional basis than in most - possibly all - other EU Member States; the DPA98 would appear to fall short of EC Directive 95/46/EC in many respects; and the Government is proposing to allow data sharing on terms that are likely to violate European law; but the UK data protection authority, the *Information Commissioner's Office* (ICO), feels not called upon to address that latter issue, even though the Information Commissioner himself warned in 2004 that that Britain was 'sleepwalking into a surveillance society',[15] and added in 2006 that we had woken up in one.[16]

1.2. Overview of data protection laws, -regulations and -institutions

[45]. The *Data Protection Act 1998 (DPA)*,[17] which replaced the previous UK data protection law, the *Data Protection Act 1984*,[18] and which was adopted in order to implement Directive 95/46/EC, came into force on 1 March 2000, together with a large number of Statutory Instruments, which provide additional detailed regulation.

---

before it could be implemented. However, neither the outcome of the consultation nor the ICO report would be binding, and ministerial orders placed before Parliament are rarely, if ever, rejected: in the UK, this is an extremely weak safeguard. Yet once in force, such orders would override any restrictions in the DPA. It may be noticed that the ICO report would in any case not address the question of compatibility of a proposed order with the ECHR or the EC Directives: see para.41 of this report.

14 'Lords Constitution Committee to investigate impact of surveillance and data collection', House of Lords Press Notice, 26.04.2007, available at: http://www.parliament.uk/parliamentary_committees/lords_press_notices/pn260407const.cfm (26.01.2009).

15 'Watchdog's Big Brother UK warning', BBC News, 16.08.2004, available at: http://news.bbc.co.uk/1/hi/uk_politics/3568468.stm (26.01.2009).

16 See: http://news.bbc.co.uk/1/hi/uk_politics/3568468.stm (26.01.2009).

17 UK/Data Protection Act 1998 c.29 (16.07.1998), available at: http://www.opsi.gov.uk/Acts/Acts1998/ukpga_19980029_en_1 (26.01.2009).

18 UK/Data Protection Act 1984 c.35 (repealed 01.03.2000), available at: http://www.opsi.gov.uk/RevisedStatutes/Acts/ukpga/1984/cukpga_19840035_en_1 (26.01.2009).

[46]. The UK has since adopted the *Privacy and Electronic Communications (EC Directive) Regulations 2003*[19] and the *Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2004*,[20] to implement Directive 2002/58/EC.

[47]. Directive 2006/24/EC on the retention of telecommunications data has not (yet) been implemented by means of a law. Instead, the UK is relying on a *Code of Practice on Data Retention* approved by Parliament in December 2003 in the form of the *Retention of Communications Data (Code of Practice) Order 2003*[21] (but which does not have force of law), and on certain informal, supposedly voluntary measures adopted by a number of the UK's Internet Service Providers (ISP), under which the latter retain the relevant data.[22] This is problematic because it means the data retention is not based on a 'law' in the European (ECHR) sense.

[48]. Mention must also be made in this context of the *Regulation of Investigatory Powers Act 2000*[23] (RIPA), which allows widespread access to communications data by public authorities (and which has also been criticised as being in violation of European [EC- and ECHR-] law).[24]

[49]. It is a typical feature of data protection law in the UK that many matters are addressed not in formally binding rules or regulations, but in non-binding 'legal guidance', 'codes of practice', 'guidance notes', 'good practices notes', 'technical guidance notes', and simpler leaflets directed at the general public issued by the ICO. The UK Ministry of Justice has also issued *Guidance for professionals and practitioners on [the] application of the Data Protection Act 1998*,[25] in the form of a series of leaflets.

---

19 UK/The Privacy and Electronic Communications (EC Directive) Regulations 2003 SI 2426 (11.12.2003), available at: http://www.opsi.gov.uk/si/si2003/20032426.htm (26.01.2009).

20 UK/ The Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2004 SI 1039 (25.06.2004), available at: http://www.opsi.gov.uk/si/si2004/20041039.htm (26.01.2009).

21 UK/The Retention of Communications Data (Code of Practice) Order 2003 SI 3175 (05.12.2003), available at: http://www.opsi.gov.uk/si/si2003/20033175.htm (26.01.2009).

22 For details and a critical analysis, see I. Brown (2009) *Regulation of converged communications surveillance*, Oxford Internet Institute, p. 8ff.

23 UK/The Regulation of Investigatory Powers Act 2000 c.23 (28.07.2000), available at: http://www.opsi.gov.uk/acts/acts2000/ukpga_20000023_en_1 (26.01.2009).

24 See I. Brown (2009) *Regulation of converged communications surveillance*, Oxford Internet Institute, p. 3ff.

25 UK Ministry of Justice, *Data Sharing and Protection. Guidance for professionals and practitioners on application of the Data Protection Act 1998*, available at: http://www.justice.gov.uk/guidance/datasharing.htm (26.01.2009)

2. Data Protection Authority

2.1. General (name & legal basis, type/structure, staffing & budget)[26]

[50]. The UK data protection supervisory authority, established under the *Data Protection Act 1998*, was originally called the 'Data Protection Commissioner' (s.6(1) DPA98).[27] In 2001, it was renamed the Information Commissioner after it was also, separately, charged with supervision over the UK *Freedom of Information Act 2000*[28] (s.18(1) FOIA). In practice, and on its own website, the authority is referred to as the *Information Commissioner's Office* or ICO.[29]

[51]. The Information Commissioner is appointed for a term of five years, and can be re-appointed twice, serving a maximum term of office of fifteen years (s.2(1) and 2(4) Schedule 5, DPA98). He may be relieved of his office by the Government at his own request (s.2(2) Schedule 5 DPA98) or may be removed by Government following an Address from both Houses of the Parliament (s.(2(4) Schedule 5, DPA98).

[52]. In addition to the Commissioner, there is the *Information Tribunal* (formerly the *Data Protection Tribunal*) that can hear appeals from controllers who have been served with certain 'notices' by the Commissioner. This is further discussed in section 2.2.4, below.

[53]. In law, all the powers of the authority are vested in the Information Commissioner in person. In practice, these powers are exercised by the ICO as a body. The ICO has a Management Board, consisting of the Executive Team, which has six members including the Commissioner himself, and four Non-Executive Directors. It also has an Audit Committee, a Policy Committee, and an Operations Management Committee.[30]

---

[26] The authority's functions and powers are discussed in section 2.2, its remit in section 2.3, and the question of the authority's independence in section 2.4.

[27] Its predecessor under the *Data Protection Act 1984* was called the Data Protection Registrar.

[28] UK/Freedom of Information Act 2000 c.36 (30.11.2000), available at: http://www.opsi.gov.uk/Acts/acts2000/ukpga_20000036_en_1 (26.01.2009).

[29] See: http://www.ico.gov.uk/ (26.01.2009).

[30] See ICO (2007) *Annual Report 2006/2007*, p.55, available at: http://www.ico.gov.uk/upload/documents/library/corporate/detailed_specialist_guides/annual_report_2007.pdf (26.01.2009). For details, see: http://www.ico.gov.uk/about_us/who_we_are/management_board.aspx; http://www.ico.gov.uk/about_us/who_we_are/corporate_governance.aspx;

[54]. Unusually, for a core UK Governmental body, the ICO has its main offices far from the UK capital: it is based in Wilmslow, in Cheshire, near Manchester, some 185 miles from London. Since 2003, in response to the general devolution process in the UK, the ICO has had three regional offices, in Northern Ireland (Belfast), Scotland (Edinburgh) and Wales (Cardiff).

[55]. The number of staff of the ICO has risen from 114 in 2000,[31] through 208 in 2004,[32] to 262 in 2007.[33] Part of this is related to the fact that, from 2001, the ICO also became responsible for freedom of information. However, the number of data protection complaints dealt with in the latest year for which figures are available, 2007, are almost ten times those of the number relating to freedom of information: in that year, the ICO dealt with some 24,000 data protection complaints against 2,500 freedom of information complaints.[34] Many of the staff will be dealing with the task of processing notifications (registrations) from data controllers, if only because the ICO depends on the fees (see next paragraph), although many doubt the usefulness of the system (as further discussed in section 2.2.8, below).

[56]. The ICO's expenditure on data protection activities is financed through the retention of the fees collected from data controllers who notify their processing of personal data under the *Data Protection Act 1998*.[35] The annual notification fee is £35 (unchanged since it was introduced on 1 March 2000). The fee income collected in the year 2006/07 was £10,204,761 (2005/06: £9,655,060) representing an increase of almost 5.7% over the previous year.[36] The ICO aims to increase the number of organisations notifying the Commissioner by 2% each

http://www.ico.gov.uk/upload/documents/library/corporate/practical_application/organisational_chart.pdf (26.01.2009).

31 ICO(2001) *Annual Report 2001*, p.66, available at: http://www.ico.gov.uk/upload/documents/library/corporate/detailed_specialist_guides/annual_report_2001.pdf (26.01.2009).

32 ICO (2004) *Annual Report 2002/03*, p.80, available at: http://www.ico.gov.uk/upload/documents/library/corporate/detailed_specialist_guides/annual_report_2004.pdf (26.01.2009).

33 ICO (2007) *Annual Report 2006/07*, p.81, available at: http://www.ico.gov.uk/upload/documents/library/corporate/detailed_specialist_guides/annual_report_2007.pdf (26.01.2009). The precise figures for the years 2000 – 2007 are set out in Annex 1 to this report.

34 ICO (2007) *Annual Report 2006/7*, pp. 12 and 14, available at: http://www.ico.gov.uk/upload/documents/library/corporate/detailed_specialist_guides/annual_report_2007.pdf (26.01.2009).

35 Note that the ICO's expenditure on freedom of information is, by contrast, financed directly by the Government by means of a so-called grant-in-aid from the Department for Constitutional Affairs (DCA). For 2006/07, this grant amounted to £5,550,000 (2005/06: £5,100,000).

36 ICO (2007) *Annual Report 2006/07*, p. 62, available at: http://www.ico.gov.uk/upload/documents/library/corporate/detailed_specialist_guides/annual_report_2007.pdf (26.01.2009).

year, and therefore anticipates data protection fee income to increase to £10.4 million in 2007/08, £10.6 million in 2008/09, and £10.8 million in 2009/20.[37]

[57]. The way in which the ICO will carry out his functions and can spend this fee money is governed by a *Framework Document* between the ICO and the Department for Constitutional Affairs. The *Framework Document* comprises a *Management Statement*[38] and a *Financial Memorandum*.[39] Between them, they cover in particular:

- the rules and guidelines relevant to the exercise of the Commissioner's functions, duties and powers;
- The conditions under which any public funds are paid to the Commissioner;
- the arrangements for the Commissioner reporting to Parliament; and
- the relationship between the Secretary of State for Constitutional Affairs and his Department, and the Commissioner.

[58]. An analysis of whether the resources of the ICO are sufficient to ensure effective use of his powers is provided in sub-section 2.2.8, after a description of those powers and their use in practice.

2.2. Functions & Powers of the ICO

2.2.1. Right to be consulted on rules and regulations (Art. 28(2) of Directive 95/46/EC)

[59]. Contrary to Article 28(2) of Directive 95/46/EC, the ICO is not required to be consulted by central or other bodies when those bodies draw up 'administrative measures or regulations relating to the protection of individuals' rights and freedoms with regard to the processing of personal data.'[40] The Commissioner

[37] ICO (2007*) Corporate Plan 2007-2010 - What and how? Our strategy over the next three years*, p. 24, available at: http://www.ico.gov.uk/upload/documents/library/corporate/detailed_specialist_guides/corporate_plan_2007-2010.pdf (26.01.2009).

[38] *Framework Document for the Information Commissioner. Management Statement*, April 2005, available at: http://www.ico.gov.uk/upload/documents/library/corporate/detailed_specialist_guides/management_statement_april_2005.pdf (26.01.2009).

[39] *Framework Document for the Information Commissioner. Financial Memorandum*, April 2005, available at: http://www.ico.gov.uk/upload/documents/library/corporate/detailed_specialist_guides/financial_memo_april_2005.pdf (26.01.2009).

[40] The requirement in the *Coroners and Justice Bill* for a report by the Information Commissioner on any proposed data sharing orders, if adopted, would be an exception to this general situation.

occasionally speaks out against a particular legislative proposal. For instance, in July 2008, at the launch of his 2007 Annual Report, the Commissioner suggested that the Government plans for a specially-created database - potentially accessible to a wide range of law enforcement authorities - holding details of everyone's telephone and internet communications might be 'a step too far'.[41] He is also often consulted, e.g., on the drafting of codes of conduct for the sharing of personal data within the public sector. But Government Departments and Ministries and other relevant bodies are not required to consult him on proposed new legislation or lower level rules raising data protection issues, and they do not systematically do so.

2.2.2. Investigative powers[42] (Art. 28(3), first indent, of Directive 95/46/EC)

2.2.2.1. Search and Seizure

[60]. Different from many other Member States, in the UK the ICO does *not* have any autonomous powers of access to data, or premises, on demand, of his own motion. Under the DPA98, the Commissioner can obtain a search warrant which does give the ICO staff powers of entry and inspection - but he must apply for such a warrant to a judge, and can only do so if there are reasonable grounds for suspecting that an offence under the Act has been committed or that the data protection principles have been contravened (s.50 and Schedule 9 to the Act). Except in urgent cases (or if this would defeat the object of the search), the controller must be given a week's notice of the intended search (Schedule 9, para.2). Data relating to national security and (except in wholly exceptional circumstances) communications between a lawyer and his client are exempt from seizure (Schedule 9, para. 9).

2.2.2.2. Information Notices

[61]. The Commissioner also has the less intrusive power to issue a so-called 'Information Notice'. This is a notice requiring an organisation or person to

[41] *'...a step too far'*, ICO Annual Report Launch 15 July 2008, Extracts from the speech of Richard Thomas, Information Commissioner, available at: http://www.ico.gov.uk/upload/documents/pressreleases/2008/annual_report_2008_rt_speech.pdf (26.01.2009).

[42] The information in this sub-section is largely taken from the description of regulatory actions available to the ICO in an ICO document called *A Strategy For Data Protection Regulatory Action*, under the heading 'Forms of Regulatory Action'. The document dates from November 2005 but still reflects current policy. It is available from the ICO website at: http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/data_protection_regulatory_action_strategy.pdf (26.01.2009).

supply the Commissioner with the information specified in the notice for the purpose of assessing whether the Act or related laws have been complied with. Failure to comply with a notice is a criminal offence.[43]

[62]. The recipients of an Information Notice can appeal against the notice to a special appellate body, the *Information Tribunal*: see sub-section 2.2.4, below.

[63]. On the use of the above powers in practice, see sub-section 2.2.8.

2.2.3. Powers of Intervention[44] (Art. 28(3), second indent, of Directive 95/46/EC)

2.2.3.1. Prior Checks

[64]. The Secretary of State may specify by Order that certain kinds of processing are, in his opinion, 'particularly likely' to cause substantial damage or substantial distress to data subjects, or 'otherwise significantly to prejudice [their] rights and freedoms' (s.22(1) DPA98). Such 'particularly risky' processing operations (referred to in the Act as 'assessable processing') must be 'notified' (registered) even if the filing system used is a manual one (cf. s. 17(2) DPA98), and the processing is then subject to a prior assessment (what the Directive calls 'prior checking') by the Commissioner (s.22 DPA98).

[65]. The assessment is to determine whether, in the view of the Commissioner, the processing in question is 'likely to comply with the provisions of [the] Act' (s. 22(2)(b) DPA98). The Commissioner must make this determination within 28 (or in special cases, 42) days and no processing of this kind may take place until the expiry of this period or until a notice has been received from the Commissioner that sets out the Commissioner's views on the compatibility of the processing with the Act (s.22(3)–(5) DPA98). Contravention of this prohibition is a criminal offence (s.22(6) DPA98). The Act does not, in section 22, expressly prohibit processing of a kind that the Commissioner has determined is likely to violate the Act, but the Commissioner can (and in

[43] UK/Data Protection Act 1998 c.29 (16.07.1998), ss.43 and 44, available at: http://www.opsi.gov.uk/Acts/Acts1998/ukpga_19980029_en_1 (26.01.2009), and UK/The Privacy and Electronic Communications (EC Directive) Regulations 2003 SI 2426 (11.12.2003), Regulation 31, available at: http://www.opsi.gov.uk/si/si2003/20032426.htm (26.01.2009).

[44] The information in this sub-section is partly taken from the document *:* ICO (2005) *A Strategy For Data Protection Regulatory Action*, available at: http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/data_protection_regulatory_action_strategy.pdf (26.01.2009), and partly from the 'Country Report on the UK', issued on CD-ROM with D. Korff (2006) *Data Protection Law in Practice in the EU*, Brussels/New York.

appropriate cases, undoubtedly will) issue an 'enforcement notice' (as further discussed under the next sub-heading) to ensure compliance with his views.

[66]. However, no Order has as ever been issued in which any types of processing operations were designated as 'risky' in the above sense. The previous Commissioner was of the opinion that 'no 'assessable processing' should be designated,'[45] and the current Commissioner has also not called for it. In practice, therefore, the system of 'prior checks' envisaged in the Directive, while in theory available, is not actually used in the UK at all.[46]

2.2.3.2. Enforcement Notices (= orders)

[67]. The Commissioner can issue so-called 'Enforcement Notices'. These are formal notices requiring an organisation or individual to take the action specified in the notice in order to bring about compliance with the Act and related laws. This can typically include correcting, blocking, erasure or destruction of data. Failure to comply with a notice is a criminal offence (s.40 DPA98 and Regulation 31 *Privacy and Electronic Communications (EC Directive) Regulations 2003*). An Enforcement Notice can also be used to order a controller not to take certain actions, or to cease them; in that case, the ICO refers to the notices as 'Stop Now Orders' (but that is not a formal term).

[68]. The recipients of an Enforcement Notice, too, can appeal against the notice to the *Information Tribunal*: see sub-section 2.2.4, below.

[69]. In fact, although there is no specific basis for this in the Act, the ICO only rarely resorts to Enforcement Notices, and instead relies more on 'encouraging' compliance in other, less forceful ways such as requiring controllers to sign an undertaking, as will be discussed in sub-section 2.2.7.

[70]. On the use of the above powers in practice, see sub-section 2.2.8.

---

[45] UK Ministry of Justice (2001) *Data Protection Act 1998: Post-Implementation Appraisal. Summary of Responses to September 2000 Consultation*, Part B Comments of the Information Commissioner, Section 22, available at: http://www.dca.gov.uk/ccpd/dparesp.htm#part14 (26.01.2009).

[46] More than a decade ago, *Justice* (the British Section of the International Commission of Jurists) suggested that appropriate categories to be designated as 'risky' would be data matching and the use of CCTV cameras. See: Justice (1998) Briefing on the Data Protection *Bill for its Second Reading in the House of Lords*, available at: http://www.justice.org.uk/parliamentpress/parliamentarybriefings/index.html (26.01.2009). But the issue has largely disappeared from the debate since then.

2.2.3.3. Lesser Measures

[71]. As noted, in practice, the ICO rarely resorts to the issuing of Enforcement Notices. The Commissioner and his staff prefer to first raise the issue with any person or organisation concerned, and attempt to resolve the matter 'by negotiation or other less formal means'.[47] Such 'negotiated resolutions' can be backed by a formal undertaking given by an organisation to the Commissioner. This can perhaps to some degree be equated to the 'warning or admonishing [of] the controller', mentioned in Article 28(3), second indent, of the Directive, although the process is in fact more like a discussion than a one-way warning.[48]

[72]. On the use of the above 'soft measures' in practice, see sub-section 2.2.8. On the use of tougher, criminal sanctions, see section 2.2.5.

2.2.3.4. Reports to Parliament

[73]. Under s.52 of the DPA98, the Information Commissioner must submit annually to Parliament 'a general report on the exercise of his functions under this Act.' (s.52(1)). He may also submit to it 'such other reports with respect to those functions as he thinks fit' (s.52(2)); and he must also submit any sectoral code of practice to Parliament, when it is a code that the Secretary of State has ordered to be drawn up (s.52(3)).

[74]. The ICO Annual Reports cover all the various activities of the office. The 'other reports' tend to address broad issues[49] or (as more specifically indicated in s. 52(2)) matters relating to the Commissioner's functions or powers (such as the power to carry out audits without being asked to, as discussed in section 2.2.6). These provisions are not really used in the manner suggested by Article 28(3) of the Directive, which speaks of the national supervisory authority 'referring [a specific] matter to national parliaments or other political Institutions': in the

---

47 Under the DPA84, the Data Protection Registrar (as the authority was then called) used to issue 'preliminary' notices, warning controllers (or data users as they were then called) that they would be served with a real notice unless they changed their practices: see D. Korff (1997) *EC study on Existing Case-Law on Compliance with Data Protection Laws and Principles in the Member States of the European Union*, pp. 20 – 23. However, this no longer appears to be done.

48 Controllers who have committed a criminal offence under the DPA98 may, instead of being prosecuted, be given a 'caution', but such cautions are, in the UK, in fact actual sanctions, and not just 'warnings or admonitions'. On criminal sanctions under the DPA98, see section 2.2.5, below.

49 For example, in May 2006, the Information Commissioner presented the report '*What Price Privacy?'* to Parliament. The report called for the government to introduce a custodial sentence for individuals convicted under the *Data Protection Act 1998* for unlawful obtaining, buying and selling of personal information. See: ICO (2006) *What price privacy? The unlawful trade in confidential personal information*, available at: http://www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/what_price_privacy.pdf (26.01.2009).

context in which this is said, that would appear to envisage the authority referring specific cases of non-compliance to such institutions. In the UK, that is not done, probably because it would be considered more appropriate for such matters to be dealt with by the courts.

[75]. However, there is currently a proposal before Parliament (contained in the *Coroners and Justice Bill*) that would require the ICO to produce a report to Parliament when a Ministerial information-sharing order is introduced. This is a new kind of order, relating to controversial proposals to allow more widespread (in effect, almost limitless) data sharing in the public sector in particular.[50] The ICO has welcomed this proposal in the following terms, saying it would 'preferably' submit such a report after a privacy impact assessment has been undertaken. The ICO adds: 'Our report will address the proportionality of the information sharing and its effect on individuals. It will allow us to ensure that safeguards are in place and that individuals' rights are respected. Where appropriate, we will be able to advise Parliament that a particular initiative is a step too far, or that further safeguards are required.'[51]

2.2.4. The Information Tribunal & other (further) appeals

[76]. Controllers must comply with any Information- or Enforcement Notices served upon them by the Commissioner (s.47(1) of the DPA98). Failure to comply is a criminal offence: see section 2.2.5, below. However, the issuing of a notice is subject to a right of appeal to a special appellate body, the *Data Protection Tribunal* (ss. 48 and 49 DPA98).[52] The chairperson and deputy chairpersons are appointed by the Lord Chancellor; other members are appointed by the Secretary of State (s.6(4) DPA98). The Tribunal currently has one chairman and 13 deputy chairpersons; all are solicitors or barristers with at least 7 years professional experience. In addition, there are currently 34 non-legal members of the Tribunal. The latter are chosen because of their experience in work with data controllers or in representing data subjects.[53] For some reason, neither the ICO's nor the Department for Constitutional Affairs' (the Lord Chancellor's department), nor the (new) Ministry of Justice's websites provide any information on the terms of appointment of the Tribunal members.

---

50 See footnote 13 above.

51 ICO (2009) *Coroners and Justice Bill: A commentary from the Information Commissioner's Office – Second Reading 26 January 2009*, available at: http://www.ico.gov.uk/about_us/news_and_views/current_topics/cj_bill_commentary.aspx (26.01.2009).

52 The *Information Tribunal* used to be the Data Protection Tribunal under the DPA84.

53 See: Tribunals Service – Information Tribunal, available at: http://www.informationtribunal.gov.uk/aboutus.htm . There is also an Information Tribunal User Group (ITUG), which has the aim 'to provide an opportunity for [users of the Tribunal, i.e. data controllers] to discuss matters relating to [the Tribunal's] non case specific, operations and processes with representatives from [the] Tribunal judiciary and administration.' (idem.).

[77]. The Tribunal can review all aspects of the Commissioner's decision to issue a notice: it can review the facts (and reach different views on them) (s.49(2)), and it can substitute its own ruling for the Commissioner's, either because it feels the Commission erred in law (typically, if they disagree about the legal interpretation of a term or issue in the Act), or because they feel the Commissioner should have exercised any discretion he may have had differently (s.49(1)).

[78]. It should be noted that data subjects do not have a right to bring cases (or Commissioner's rulings) affecting them to the Tribunal. Indeed, they are not party to (or otherwise given any standing in) any cases before the Tribunal: their interests are supposed to be served by the Information Commissioner.[54]

[79]. Since the coming into force of the DPA98, there have been only nine cases decided by the Tribunal in which reference was made to that Act: One in 2000, one in 2005, four in 2007, and three in 2008.[55] However, the main issue in several of these, including the only one appealed to the High Court, in fact related to the *Freedom of Information Act 2000* (FOI Act).[56] There were only three cases that only concerned the DPA98. An appeal (to the Court of Appeal) is still pending in the latest case, relating to retention of personal information on the Police National Computer (PNC). It is notable that the Tribunal, by contrast, has issued 166 decisions under the FOI Act, under which individuals as well as organisations can appeal to it, even though it has had jurisdiction under that Act for a shorter period.[57]

[80]. Controllers can appeal from a ruling of the Tribunal to the High Court (in England; in Scotland, the appeal lies with the Court of Sessions, and in Northern Ireland with the Northern Irish High Court) (s.49(6) DPA98). However, these appeals are limited to points of law only. Under English law this does include the possibility to challenge a decision by an administrative body that was manifestly unreasonably, failed to take relevant matters into account or took matters into account that were not relevant - but it will be very rare indeed for that to apply to a Tribunal ruling.

---

54 Because of this, data subjects are not 'users' of the Tribunal's services and, hence, not given access to the Information Tribunal User Group mentioned in the previous footnote.

55 Full list of decisions available at: http://www.informationtribunal.gov.uk/Public/search.aspx (26.01.2009). Select 'Data Protection Act 1998' in the box marked 'jurisdictional area'. The two results pages list a further 11 earlier cases as relating to the DPA98, but in fact these were all decided under the DPA84 (although points of law etc. will usually be equally applicable under the new Act).

56 UK/Freedom of Information Act 2000 c.36 (30.11.2000), available at: http://www.opsi.gov.uk/Acts/acts2000/ukpga_20000036_en_1 (26.01.2009).

57 See the list of decisions under the FOI Act at: http://www.informationtribunal.gov.uk/Public/search.aspx (26.01.2009). Select 'Freedom of Information Act 2000' in the box marked 'jurisdictional area'.

[81]. One very important case that was decided by the higher courts was the case of *Durant v Financial Services Authority*.[58] In that case, the Court of Appeal explicitly gave a *narrow* interpretation to the crucial term 'personal data' - in direct contrast to the 'constitutional' approach to data protection taken in other EU Member States and by the European courts, which all give the term a *broad* interpretation - resulting in greater protection for the individual.[59] The case thus illustrates the problem of the lack of a constitutional basis for data protection in the UK (as discussed in section 1.1, above) and the related - indeed, partially consequent - problem that the courts in the country are disinclined to give strong protection to personal information and privacy. It combines with the overall relatively weak enforcement of the DPA98 by the ICO, as discussed in section 2.2.7, below, to create a data protection regime in the UK that is notably less-developed, and weaker, and less enforced, than the data protection regimes in other EU Member States.

2.2.5. Powers to engage in [criminal] legal proceedings (Art. 28(3), third indent, of Directive 95/46/EC)

[82]. The DPA98 sets out a number of criminal offences, most of them carried over from the previous law, the DPA84. Most of them concern action, or failure to

[58] *Durant v Financial Services Authority* [2003] EWCA Civ 1746. Cf. the following passage from the CA judgment: 'In conformity with the 1981 Convention and the Directive, the purpose of section 7 [DPA98], in entitling an individual to have access to information in the form of his "personal data" is to enable him to check whether the data controller's processing of it unlawfully infringes his privacy and, if so, to take such steps as the Act provides, for example in sections 10 to 14, to protect it. It is not an automatic key to any information, readily accessible or not, of matters in which he may be named or involved. Nor is to assist him, for example, to obtain discovery of documents that may assist him in litigation or complaints against third parties. As a matter of practicality and given the focus of the Act on ready accessibility of the information - whether from a computerised or comparably sophisticated non-computerised system - it is likely in most cases that only information that names or directly refers to him will qualify. In this respect, *a narrow interpretation of 'personal data' goes hand in hand with a narrow meaning of 'a relevant filing system'*, and for the same reasons (…).' (para. 27 of the judgment, emphasis added). The Court of Appeal then goes on to say, in effect, that even readily available information need not be covered, unless it infringes privacy.

[59] Rather than data protection having to be narrowly applied to matters deemed to be strictly 'private' (as the Court of Appeal ruled), the European Court of Human Rights goes the other way: it extends the concept of 'private life' to fit in with the new, wider concept of data protection. As the Court puts it: its recent case-law 'emphasise[s] the correspondence of this *broad* interpretation [of Art. 8 of the Human Rights Convention] with that of the [Data Protection Convention].' Cf. also the comments in the Explanatory Memorandum to the Council of Europe Convention on data protection that the concept of 'privacy' as used in that instrument ' is not to be interpreted simply in terms of protection of one's private sphere against intrusive conduct' but rather 'goes beyond traditional privacy notions' (paras. 17 and 19).

act, in relation to notification or in relation to measures taken in the course of supervision or enforcement.[60]

[83]. In England and Wales and Northern Ireland, criminal proceedings for these offences can be instituted by the Information Commissioner or by others (such as a Government Department or indeed a private individual or company). However, any of these first require the consent of the Director of Public Prosecutions (in Northern Ireland, the DPP for Northern Ireland) (s.60(1) DPA98). In Scotland, prosecutions will normally be brought by the Procurator Fiscal (the equivalent to a public procurator on the Continent).

[84]. If the ICO, or more precisely the prosecuting authority acting at the instigation of the ICO, feels that the matter can be dealt with without an actual prosecution, they can 'caution' a person accused of one of the offences under the Act. A caution is a formal procedure in English law, which does constitute a formal criminal *sanction*, even if it may not amount to a full criminal *conviction*.[61] Receiving a formal caution from a prosecution authority is therefore a much more serious matter than merely receiving a 'warning or admonition' from a data protection authority (of the kind apparently envisaged in Article 28(3) of the EC Directive).

[85]. On the use of the above powers in practice, see sub-section 2.2.7.

2.2.6. Audit powers (Art. 28(3), third indent, of Directive 95/46/EC)

[86]. According to s.51(7) of the DPA98, 'The Commissioner may, with the consent of the data controller, assess any processing of personal data for the following of good practice and shall inform the data controller of the results of the assessment.' This is seen as the (sole) basis on which the Commissioner can currently carry out audits of controllers' personal data processing operations.[62]

---

60 For the full list, see section 4 of this report on 'Sanctions, Compensation and Legal Consequences'.

61 There is in fact some confusion over this. Thus, the Home Office says: 'A simple caution is not a criminal conviction, but it will be recorded on the police database. It may be used in court as evidence of bad character, or as part of an anti-social behaviour order (ASBO) application.' See: http://www.homeoffice.gov.uk/police/powers/cautioning/ (26.01.2009). However, a police form used to issue the caution, quoted in *Jones v. Whalley* [2006] UKHL 41, and which the Lords seemed to accept as correct, says: 'WHAT A CAUTION MEANS TO YOU: The record of caution is a criminal conviction which is citable in a court should you re-offend.' See: http://www.publications.parliament.uk/pa/ld200506/ldjudgmt/jd060726/whall-1.htm. (26.01.2009).

62 Under s. 42(1) of the Act, 'A request may be made to the Commissioner by or on behalf of any person who is, or believes himself to be, directly affected by any processing of personal data for an assessment as to whether it is likely or unlikely that the processing has been or is being carried out in compliance with the provisions of this Act.' The article continues in the

However, as the provision stresses, the Commissioner does not have the power to demand that he be allowed to carry out an audit of his own motion. Because of this, in practice, audits are still relatively rare; in the year 2006-07, the ICO carried out eight audits of processing operations of public bodies, at the request of those authorities.[63]

[87]. A Bill currently before Parliament, the *Coroners and Justice Bill*, mentioned above, if adopted, will remedy this to some extent, in that it will, for the first time in the UK, allow the data protection authority to order an audit. However, the proposed new power is still limited in scope and practical ways, and has been criticised by the Information Commissioner in the following terms:

'As it stands, the Bill will allow the ICO to serve an assessment notice on a government department or a designated public authority. The Bill would not, though, allow the ICO to serve an assessment notice on a private or third sector organisation.

Particular risks can arise in public sector contexts. Individuals may be required by law to provide very sensitive information to organisations with very extensive collections of records. Therefore we are pleased that the Bill gives us a power to serve an assessment notice on government departments and designated public authorities. We are concerned, though, as to how far our power will ultimately reach.

The level of risk that arises in private sector contexts should not be underestimated. The line of demarcation between the public and other sectors is becoming increasingly blurred. Private and third sector bodies frequently carry out work for public sector ones. **It is common for charities, for example, to carry out functions on behalf of local government. As it stands, we could inspect the local authority, but not the charity**.

Some private sector bodies hold enormous amounts of sensitive information about large parts of the population. Individuals may have no alternative to providing information to them. For example, an application for credit will necessarily involve information about a person's finances being shared between the credit reference agencies. The loss, corruption or misuse of private sector information can be extremely damaging. Most will be are aware of the severe consequences for individuals when they are "locked out" of their bank-

---

next paragraph, by stipulating that 'On receiving a request under this section, the Commissioner shall make an assessment in such manner as appears to him to be appropriate'. However, this assessment in response to an individual complaint is not regarded as analogous to an assessment under s. 51(7), and is not used by the ICO to carry out an audit of the controller's processing operations in the manner envisaged in that latter section, as discussed in the text.

63 ICO (2007) *Annual Report 2006-07*, p.25, available at: http://www.ico.gov.uk/upload/documents/library/corporate/detailed_specialist_guides/annual_report_2007.pdf (26.01.2009).

accounts, have their electricity turned off due to an "administrative error" or become the victims of identity fraud.

We have no desire to undertake heavy handed or widespread inspections. We only take action where we identify a specific risk to individuals, for example by analysing the tens of thousands of complaints that we receive each year – most of which are about private sector organisations. **We are strongly of the view that if individuals are to be protected properly, we must be able to serve assessment notices on all organisations**.

It is particularly worrying that the Bill does not provide for any sanction if an assessment notice isn't complied with, but does provide for a formal right of appeal against a notice. In order to make our power of inspection effective, and to ensure the credibility of the inspection process, even if it is limited to public bodies, there must be a sanction where an organisation fails to comply with an assessment notice. One approach would be to introduce a clause similar to s.54 of the *Freedom of Information Act 2000*. This treats failures by public authorities to comply with our FOI notices as a contempt of court.'[64]

2.2.7. The use of the ICO's powers in practice - a critical assessment

[88]. In the year covered by the *2006-07 Annual Report*, the ICO dealt with approximately 24,000 data protection cases.[65] The first point that should be made is that these are the cases that were specifically brought to the attention of the ICO - mostly through complaints from data subjects, or perhaps as a result of press reports or concern expressed in Parliament. It is crucial to note early on that the ICO does **not** go out of his way to try and uncover breaches of the Act unless they somehow become exposed.

[89]. This is most obvious from the figures relating to notification (registration). Under the DPA98, all controllers of automated processing operations are required to notify the Commissioner of their operations (ss.17(1) and (2) DPA98). This is subject to some exceptions, but even if one takes those into account, a close reading of the Act would mean that the vast majority of companies and organisations (and indeed quite a few individuals) should register. But it has long been clear that many - probably most - simply do not

[64] ICO (2009) *Coroners and Justice Bill: A commentary from the Information Commissioner's Office – Second Reading 26 January 2009*, available at: http://www.ico.gov.uk/about_us/news_and_views/current_topics/cj_bill_commentary.aspx (26.01.2009).Original emphasis in bold.

[65] ICO (2007) *Annual Report 2006/07*, p. 13. See also footnote 66, below. Note that these are only the cases received in writing; the ICO also dealt with 'more than 115,000 telephone enquiries, of which more than 80% [i.e., some 92,000 – DK] were about data protection'. See ICO (2007) *Annual Report 2006/07*, p. 21.

register. Estimates from the mid-90s varied between one- and two-thirds of all controllers who should register failing to do so. Early research by the then Data Protection Registrar, reported in her *1996 Annual Report*, suggested that even of those businesses that were aware of their registration duties, only 14 – 15% had actually done so.[66]

[90]. Although the number of registrations has greatly increased, to some 287,000 in 2006-07 (it was only about 100,000 in the mid-90s), this will partly be due to the increase in the numbers of companies since then, and partly to the increase in the use of computers, also by small companies. In 2006-07, there were more than 2.3 million companies registered with Companies House (the UK Government body registering them), up from 1.8 million in 2003-04.[67] This already excludes companies in liquidation or in the process of removal from the register, but even if one accepts that some will not be actively trading, it still cannot be the case that only 300,000, or some 12% needed to register. On the contrary, even at a very conservative guess, one would assume that at the least 80% of active businesses use IT processes that involve processing of personal data that they should register. Clearly, the majority of companies still do not register, even if they have to. This may account for perhaps as many as 1 – 1.5 million unreported and undetected breaches of the Act.

[91]. This is not, however, a matter that is very actively pursued by the ICO, at least not in terms of enforcement action.[68] If the Commissioner hears that a company has not registered, and feels that it perhaps should, he reminds the company of this duty. It is only if a controller consistently and deliberately ignores repeated entreaties and warnings that the Commissioner's staff resort to stronger measures. In the year 2006-07, they brought just 10 prosecutions for non-registration, under s. 17 of the DPA98. This is perhaps not surprising, given on the one hand the general disillusion with notification as a means of encouraging compliance (as further discussed in section 2.2.8), and on the other hand the

---

66 For details, see D. Korff (1997) *EC study on Existing Case-Law on Compliance with Data Protection Laws and Principles in the Member States of the European Union. Interim Report*, p.17ff. That report notes that this problem is far from limited to the UK: non-registration is just as bad in other countries, such as the Netherlands and France.

67 Companies House (2008) *Statistical Tables on Companies Registration Activities 2007-08*, p. 3, available at: http://www.companieshouse.gov.uk/about/pdf/companiesRegActivities2007_2008.pdf (26.01.2009).

68 In the year 2005-06, the ICO did take some action, in that it wrote to (all?) firms of solicitors and accountants that had not notified the ICO that they were processing personal information - presumably on the presumption that it would be impossible for such firms to operate without processing personal data. This led to increases in notifications of 19% for each of these sectors compared to 2004-2005. See ICO (2006) *Annual Report 2005-06*, p. 30, available at: http://www.ico.gov.uk/upload/documents/library/corporate/detailed_specialist_guides/annual_report_2005.pdf (26.01.2009). But there is no information on whether, and if so how and to what extent, those firms that still did not notify their operations were pursued; it would appear that the ICO marked the increase in notification as a success, and left it at that.

pretty minor results: all defendants were fined sums between £75 and £300.[69] With these kinds of penalties, it is not surprising that many companies simply take their chances, and only register when caught out and told to do so.

[92]. The problem is that one must assume that if controllers do not even register, it is likely they will also not take their other, more onerous duties under the Act seriously; indeed, it will be more difficult to notice other possible failures. It is therefore extremely likely that the 24,000 cases that were dealt with by the ICO represent no more than the proverbial 'tip of the iceberg'. This is the more so since, as we shall see, the cases that are pursued tend to revolve around failure to notify, unsolicited marketing, and persistent criminal obtaining and selling of information - in other words, they constitute what American politicians call 'low-hanging fruit'. More intricate matters, such as whether proper consent is obtained for certain processing operations, or whether data sharing is based on a sufficiently specific legal provision, or whether data are retained for longer than necessary, or used for incompatible secondary purposes other than direct marketing, are (as far as can be gleaned from the ICO's reports) not the subject of enforcement action - rather, the ICO prefers to 'consult', 'advice' and 'encourage good practice' in these areas, without addressing 'legalistic' questions in too much detail.

[93]. Even some serious, high-profile matters, over which deep concern is expressed at the European level, are only half-heartedly pursued, if at all. To take just three examples: the SWIFT and PNR (airline passenger data) issues, and the question of collecting and retaining by the police of DNA samples from arrested persons.

[94]. On the first, SWIFT, the Information Commissioner reported as follows:

'In June 2006 we, along with several data protection authorities in the EU and worldwide, received a complaint about alleged covert disclosure of information relating to European Union nationals by the Society for Worldwide Interbank Telecommunication (SWIFT). SWIFT is an international financial messaging service which connects institutions engaged in international financial transfers. The messages include information such as names and account numbers. The messaging process involves a transfer of information to the United States. According to the complainant, the United States Treasury had issued a number of administrative subpoenas to access this information as part of investigations into terrorist activity. The possibility that United States authorities had been given access to information about UK citizens generated a great deal of media coverage.

[69] See the chart in the ICO *Annual Report 2006-07*, pp. 56 - 57. Prosecutions are further discussed below, where it is noted that there appears to be one further case, not included in the chart, resulting in a fine of £1.750.

To investigate the complaint, we have maintained close contact with other data protection authorities. In November 2006, the Article 29 Working Party issued an opinion saying that the transfer of information to the US authorities had been undertaken in a manner contrary to fundamental data protection principles. It called for steps to be taken to ensure that even when investigating matters as serious as terrorism, the fundamental rights of citizens were respected.'[70]

[95]. Yet what was the actual ICO's response? Apart from 'continu[ing] to work with our European colleagues, as well as with SWIFT, to achieve this aim' (respect for the fundamental [data protection] rights of EU citizens), it appears to have been limited to the following:

'We have asked United Kingdom financial institutions to consider what steps are needed to make sure they comply with data protection legislation.' (idem)

[96]. This is all the more worrying since it is extremely likely that many other financial institutions in Europe - and in the UK, which claims to have, in London, one of the world's leading financial centres - also operate 'mirrors' of their databases outside the EU, and in the USA in particular. Indeed, this is likely to be the case also for many international, especially US-owned or affiliated corporations with major operations in the UK. Whether this is indeed the case, and if so, on what scale illegal transfers occur, is simply not investigated.

[97]. The second issue 'flagged' at the European level concerns the compulsory disclosure, under US law, to US authorities, of excessive 'PNR' data on EU airline passengers. The European data protection authorities declared these disclosures, too, to violate European data protection law, and the main EC data protection directive in particular. Yet again, there is no reference in the ICO *Annual Report 2006-07* of any action taken, or even any investigation started, in respect of the disclosure of such data by UK-based airlines. The only mention of the issue in the report is in a section on European co-operation (in a paragraph focussing on 'Third Pillar' co-operation), where the Commissioner says that that co-operation also helped the ICO 'to provide evidence as part of parliamentary scrutiny of the proposed Data Protection Framework Decision, the United States/Europe Passenger Name Records agreement and the Treaty of Prum.'[71] In contrast to the SWIFT case, UK carriers appeared not even to have been asked 'to consider what steps are needed to make sure they comply with data protection legislation.'

[98]. The issue of the taking and retaining of DNA samples from arrested persons by the police in the UK is long-standing. In 2001, the ICO said that he was 'concerned that there continues to be increasing pressure for the wider forensic use of genetic information in the form of DNA profiles,' and about new

[70] ICO (2007) *Annual Report 2006/07,* p.29.
[71] ICO (2007) *Annual Report 2006/07,* p.29.

statutory powers for their retention.[72] In 2002, after those new powers had nevertheless been adopted, he said that 'The removal of the previous statutory requirement on the police to delete fingerprint and DNA profile information where an individual is found not guilty (*Criminal Justice and Police Act 2001*[73]) causes particular concern.' He had been 'in discussions with the police service, central government and the Forensic Science Service about the intention to extend the retention periods relating to this data.'[74] In 2003, he said that fundamental values of personal privacy and public openness could not 'simply be abandoned against claims of progress and opportunity – whether widespread data sharing or intrusive telephone marketing in the name of improved customer service or excessive DNA profiling in the name of crime detection.'[75] Discussions continued, in which he raised yet more 'concerns' that, following removal of the statutory requirement for deletion, the Government wanted to go further, to allow the police to take DNA samples and fingerprints from all those arrested and retain these whatever the outcome of the case.[76] In the reports for 2002-03 and 2003-04, however, no further mention is made of the issue - which is ironic, because in August 2004, two young persons who had been arrested in 2001 and had their DNA taken and stored even after the prosecution was dropped (in one case) or the data subject had been acquitted (in the other) had taken their case to the European Court of Human Rights in Strasbourg. Their cases had gone through the UK courts between 2002 and 2004, but for some reason are not mentioned in the ICO Annual Reports for those years, or for the years 2004-05, 2005-06, or 2006-07. The latter two reports do refer to submissions on the issue of DNA retention to Parliamentary consultations in Scotland (which has its own devolved Parliament), but without providing details of those submissions, other than noting that they had been 'taken into account' by the Scottish Parliament.[77] The only other reference to DNA is in the paragraph on 'Third Pillar' European co-operation in the 2006-07 report mentioned earlier, where the report simply mentions that the *Prüm Treaty* 'provides for greater criminal justice co-operation, including the sharing of DNA profiles.'[78] The applications to the European Court of Human Rights resulted in a major, unanimous Grand Chamber judgment in December 2008, in which the Court held that the rules on DNA data retention in the UK violated

---

72 ICO (2001) *Annual Report 2000/01,* p.21, available at: http://www.ico.gov.uk/upload/documents/library/corporate/detailed_specialist_guides/annual_report_2001.pdf (26.01.2009).

73 UK/ Criminal Justice and Police Act 2001 c.16 (11.05.2001), available at: http://www.opsi.gov.uk/Acts/acts2001/ukpga_20010016_en_1 (26.01.2009).

74 ICO (2002) *Annual Report 2001/02,* p.10-11, available at: http://www.ico.gov.uk/upload/documents/library/corporate/detailed_specialist_guides/annual_report_2002.pdf (26.01.2009).

75 ICO (2003) *Annual Report 2002/03,* p.7, available at: http://www.ico.gov.uk/upload/documents/library/corporate/detailed_specialist_guides/annual_report_2003.pdf (26.01.2009).

76 ICO (2003) *Annual Report 2002/03,* p.19.

77 ICO (2006) *Annual Report 2005/06,* p.34, and ICO (2007) *Annual Report 2006/07,* p.43.

78 ICO (2007) *Annual Report 2006/07,* p.29.

Article 8 of the European Convention on Human Rights.[79] This means that the law in the UK (or at least in England) in this respect will have to be amended. But it is notable that for all the 'concern' expressed by the ICO, this has had to brought about by the Strasbourg Court, and was not the result of ICO enforcement action. Quite simply, while the rules allowing for excessive retention had not yet been cast in legislative concrete, the Information Commissioner had not tried to impose restrictions, but rather (unsuccessfully) tried to prevent them from being adopted by expressing concern and making submissions; and once that had failed, and the rules that violated the Convention had been enshrined in law (at least in England), he seemed to have felt that it was no longer within his remit to try to argue against them, and outside his powers to act against them.

[99]. The Information Commissioner, and his predecessors, all stress that even in the few cases that are pursued, they see 'hard' enforcement as a last resort: they prefer, where possible, to guide and advice, and to negotiate rather than to impose a solution. As it is put in the ICO's basic strategy document:

'We will put in place systems to ensure that Regulatory Action we take is in proportion to the harm or potential harm done. We will not resort to formal action where we are satisfied that the risk can be addressed by negotiation or other less formal means.'[80]

[100]. This reluctance to resort to formal enforcement measures is reflected in the statistics which, however, require some careful attention.[81]

[101]. Specifically, the ICO's *Annual Report 2006-07* says: 'More than half of data protection cases [that is: of the 24,000 data protection cases that were brought to the attention of the ICO – DK] required us to simply provide advice and guidance. In some cases this advice was relatively straightforward, in others extremely complex. **In the remainder of cases**, we considered whether a breach of the *Data Protection Act* or *Privacy and Electronic Communications Regulations* was likely to have occurred.'[82]

[102]. It is unfortunate that the report does not say more about the first category of cases. There seems to be a contradiction between the statement in the first sentence that these cases could be dealt with by 'simply' providing advice and

---

79 *S. and Marper v. The United Kingdom*, Application nos. 30562/04 and 30566/04, 18 December 2008, ECtHR.

80 This is still the policy. See: ICO (2005) *A Strategy For Data Protection Regulatory Action*, p.2, available at: http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/data_protection_regulatory_action_strategy.pdf (26.01.2009).

81 All statistics quoted here are from the ICO *Annual Report 2006/07*, which is the latest available. No attempt has been made to repeat the analysis over earlier years, as it is clear that the pattern is constant. Some odd aspects - in our view, defects - of the figures are noted in the text; they too equally arose in previous reports. See also section 4.2, para.147ff below.

82 ICO (2007) *Annual Report 2006/07*, p. 12, emphasis added.

guidance, and the statement in the second sentence that some of these cases were 'extremely complex'. It seems likely that there are significant numbers of cases in which specific requirements of the Act were possibly, or probably, broken, but where this was 'resolved' without going too deeply into this question, because the controller was willing to co-operate and listen to 'advice and guidance' - although in the more complex cases this will presumably have involved more of a dialogue or negotiation.

[103]. In the report, the remaining cases are put into the following main categories: 'breach likely', 'breach unlikely', and 'assessment criteria not met'. Overall, the figures (slightly simplified) break down roughly as shown in the Chart, below.

CHART: Data protection cases dealt with by the ICO 2006-07[83]

Percentage:	Numbers:	Category:
100 %	± 24,000	All data protection cases dealt with in 06-07
56 %	± 13,400	Cases dealt with through advice and guidance (apparently, without serious consideration of whether a breach of the Act had occurred)
15 %	± 3,600	Cases dealt with without serious consideration of whether a breach of the Act had occurred, because they "did not meet the assessment criteria"
12 %	± 2,900	Cases that were considered on the merits and in which it was concluded that it was "unlikely" that a breach of the Act had occurred
15 %	± 3,600	Cases that were considered on the merits and in which it was concluded that it was "likely" that a breach of the Act had occurred

[104]. The ICO does not clarify in his *Annual Report* what the 'assessment criteria' are, on the basis of which some 3,600 cases were deemed to not deserve detailed attention or regulatory action. Presumably, however, these are the criteria mentioned in the ICO's *Regulatory Action Strategy*[84] document, where this says the following:

[83] ICO (2007) *Annual Report 2006/07*.

[84] ICO (2005) *A Strategy For Data Protection Regulatory Action*, p.2, available at: http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/data_protection_regulatory_action_strategy.pdf (26.01.2009).

'In determining whether to take action, the form of any action and how far to pursue it, we will apply the following criteria:

- Is the past, current or prospective detriment for a single individual resulting from a 'breach' so serious that action needs to be taken?
- Are so many individuals adversely affected, even if to a lesser extent, that action is justified?
- Is action justified by the need to clarify an important point of law or principle?
- Is action justified by the likelihood that the adverse impact of a breach will have an ongoing effect or that a breach will recur if action is not taken?
- Are the organisation and its practices representative of a particular sector or activity to the extent that the case for action is supported by the need to set an example?
- Is the likely cost to the organisation of taking the remedial action required reasonable in relation to the issue at stake?
- Does a failure by the organisation to follow relevant guidance, a code of practice or accepted business practice support the case for action?
- Does the attitude and conduct of the organisation both in relation to the case in question and more generally in relation to compliance issues suggest a deliberate, wilful or cavalier approach?
- How far do we have a responsibility to organisations that comply with the law to take action against those that do not?
- Would it be more appropriate or effective for action to be taken by other means (e.g. another regulator, legal action through the courts)?
- Is the level of public interest in the case so great as to support the case for action?
- Given the extent to which pursuing the case will make demands on our resources, can this be justified in the light of other calls for regulatory action?
- What is the risk to the credibility of the law or to our reputation and influence of taking or not taking action?'

[105]. These criteria would appear somewhat unsatisfactory from the perspective of the individual data subject who is supposed to be the beneficiary of the Act and of the support of the ICO. Unless the ICO

feels that he or she has suffered serious detriment, or that many others are affected, or a point of principle is involved, or the organisation he or she complains of is held in bad repute, or there is a great public outcry, his or her case may well be excluded from serious attention altogether - even if 'advice and guidance' did not resolve the matter. It is clear in any case that the remaining categories - the only ones in which the ICO actually seriously considers action - cover far from all cases in which the Act was breached, and that were brought to the ICO's attention (and those may moreover be only a proportion of the overall number of cases in which the Act was breached - and a small proportion at that, if the implications of non-registration suggested earlier are correct).

[106]. Overall, therefore, it appears that the 24,000 cases brought to the attention of the ICO are only the tip of a much larger iceberg; and that, moreover, at least a proportion, perhaps even a large portion, of the 17,000 out of these 24,000 cases that are not seriously assessed with a view to determining whether the Act was breached and whether action should be taken, may also in reality consist of cases in which there were violations of the Act. This makes the figures for the remaining two categories - 2,900 cases that were considered on the merits and in which it was concluded that it was 'unlikely' that a breach of the Act had occurred, against 3,600 cases that were considered on the merits and in which it was concluded that it was 'likely' that a breach of the Act had occurred - not very meaningful.

[107]. It is nevertheless still instructive to look at what actually was done in the 3,600 cases (i) that apparently could not be dealt with 'simply' through advice and guidance - presumably, because the controller in question did not co-operate, at least not initially; (ii) that passed the 'assessment criteria'/seriousness test; and (iii) in which the ICO found a 'likely' breach of the Act. It would appear that in the vast majority of these cases the ICO still managed to persuade the controller, through negotiations, to take some form of remedial action (e.g., to correct data, or allow subject access, or improve data security). In a number of cases, including some well-publicised cases concerning banks, the controllers signed formal undertakings to carry out remedial action, such as better security measures and staff training. This avoided further action.[85]

[85] ICO (2007) *Annual Report 2006/07*,p. 24. The undertakings are listed on two pages in the ICO 'document library', together with Enforcement Notices: see http://www.ico.gov.uk/tools_and_resources/document_library/data_protection.aspx#notices; and http://www.ico.gov.uk/tools_and_resources/document_library/privacy_and_electronic_comm

[108]. It is no longer clear from the Annual Report in how many cases this involved the issuing of Information Notices.[86] The impression is that this is rare. The ICO *Annual Report 2006-07* only mentions one instance in which an Information Notice was issued in relation to a data protection issue: this was a high-profile case against a City Council (mentioned several times in the report), resulting in a conviction and a fine for the council for refusing to comply with the notice.[87] There is no indication of any other instances in which Information Notices were issued to enforce the DPA98.[88]

[109]. The absence of this information is all the more unhelpful, since the Information Commissioner himself has pointed out defects in the requirements for issuing them in the first place. In his comments on the *Coroners and Justice Bill*, he notes these and argues for better rules, as follows:

> **'**Power to require information
>
> Currently we can only serve an information notice on "the data controller". The data controller is the organisation with legal responsibility for processing personal data. The nature of modern business means that it is not always easy to determine who this is. In complex outsourcing arrangements it can be unclear who, if anyone, is ultimately in control. We need to be able to serve notices on all those involved in the processing of personal data in order to determine who the responsible data controller is.'[89]

[110]. However, the lack of clarity, in many cases, of who is the controller of a processing operation cannot be the sole reason for the lack of use of Information Notices: there must be many cases in which there are data protection issues and in which the identity of the controller is not in doubt.

---

unications.aspx (26.01.2009). The pages list 28 undertakings under the DPA98 itself, and a further 8 under the *Privacy and Electronic Communications Regulations* (PERC). Many of the former were by banks promising no longer to dispose of documents containing customers' details in rubbish bags.

86 In the past, these reports did provide statistics on the number of such notices issued in the given year, and on related matters: see the figures reproduced in D. Korff (1997) *EC study on Existing Case-Law on Compliance with Data Protection Laws and Principles in the Member States of the European Union*, pp. 21 – 22. The absence of these statistics seriously obscures the policies of the ICO.

87 The case is mentioned no less than four times: see *Annual Report 2006/07*, pp. 19, 24 (twice, once with most details and once in a highlighted box) and 57.

88 Many Information Notices were issued in relation to freedom of information requests under the *Freedom of Information Act 2000*, but that is an entirely separate matter.

89 ICO (2009) *Coroners and Justice Bill: A commentary from the Information Commissioner's Office – Second Reading 26 January 2009*, available at: http://www.ico.gov.uk/about_us/news_and_views/current_topics/cj_bill_commentary.aspx (26.01.2009).

[111]. Nor are Enforcement Notices very widely used. The ICO website provides a list of (presumably all) Enforcement Notices issued; they total 25 - 12 under the DPA98 and 13 under the *Privacy and Electronic Communications Regulations (PERC)* (mainly concerning telemarketing calls).[90] On analysis, they show that such notices were issued as follow:

- December 2006: 5 notices under PERC (2 to linked companies)
- September 2007: 1 notice under PERC
- July 2007: 2 notices under PERC
- August 2007: 4 notices under the DPA98 (to 4 police forces)
- November 2007: 1 notice under PERC and 1 under the DPA98
- January 2008: 3 notices under the DPA98
- February 2008: 1 notice under PERC
- June 2008: 1 notice under PERC
- July 2008: 2 notices under the DPA98
- September 2008: 1 notice under PERC and 1 under the DPA98
- December 2008: 1 notice under PERC and 1 under the DPA98

[112]. The ICO *Annual Report 2006-07* illustrates the policy as follows:

'The TPS and the ICO receive many complaints from individuals who have received unsolicited marketing telephone calls even though they have indicated that they do not wish to receive them.

On 5 December 2006, we issued enforcement notices against five companies who had been making unsolicited marketing calls to individuals without their consent, or to individuals who were registered with the Telephone Preference Service. The notices ordered the companies to stop telephoning individuals who had objected.'[91]

[113]. The report for that year also mentions the issuing of an Enforcement Notice to a company that was selling Electoral Register data from before 2002, when restrictions on the use of such data were brought in, and which resulted in the

[90] The notices are listed on two pages in the ICO 'document library'. See http://www.ico.gov.uk/tools_and_resources/document_library/data_protection.aspx#notices; and http://www.ico.gov.uk/tools_and_resources/document_library/privacy_and_electronic_communications.aspx (26.01.2009).

[91] ICO (2007) *Annual Report 2006/07*, p.25.

company agreeing to stop making those data available.[92] This case too resulted from 'hundreds of complaints'.

[114]. A total of six Enforcement Notices in this reporting year, and 25 in all between December 2006 and December 2008, all relating (only) to manifest abuses highlighted by 'many' or 'hundreds' of complainants, (most, under PERC, relating to unsolicited telemarketing calls) does not appear to reflect a particularly tough enforcement policy.

[115]. The same is true of prosecutions. These too are rare: In the year 2006-07, after examining the above-mentioned 3,600 cases in which a breach of the DPA98 was held to be 'likely', there were just 14 prosecutions, 11 against individuals (including two couples, with each spouse charged separately), 2 against (small) companies, and 1 against a public body (a City Council).[93] In fact, the real number of cases appears to be even smaller, in that two individuals seem to be associated with one of the firms, and three others with the other firm. So the real total seems to be just 8 cases.

[116]. What is more, the cases related to a very limited number of issues: as already noted, no less than 10 of the 14 prosecutions (in five of the eight cases) were about failure to notify (register) (s.17 of the DPA98); two of these were against small companies (each fined £300) and eight were against individuals (fined between £75 and £300). In one case, a section 17 charge was added to a main charge against an individual of unlawful obtaining etc. of personal data (s.55 DPA98); the latter was the only charge against a couple. The single individual was given a sentence of probation plus 150 hours of Community Service (i.e., compulsory unpaid work to be performed as a penalty); the spouses in the couple were given fines of £3.300 and 4.200 respectively. The remaining case concerned the conviction of a City Council for failing to comply with an Information Notice issued to uphold a complainant's right of access to her data (already mentioned). The Council pleaded guilty and was fined £300 and agreed to an audit by the ICO (it seems that it also provided the data subject with the information she demanded, although perhaps tellingly that detail is not included in the report).[94]

[117]. In addition to these actual prosecutions, five cautions were administered. In the course of the investigations, seven search warrants had been applied for - the ICO report does not reveal whether these were all granted, but it is likely that they all were. It may also be assumed that these warrants related to some of the eight cases in which subsequently a prosecution was brought.

---

92 ICO (2007) *Annual Report 2006/07*, p.24.

93 These cases are listed in a Chart in ICO *Annual Report 2006-07*, on pp. 56 – 57. Oddly, one further case is mentioned on p. 23, of a private investigator charged with unlawful obtaining of personal information (S. 55), who, it is reported there, was fined £1.750. However, that case is not included in the Chart on pp. 56 – 57 and has been left out of the analysis in the text.

94 ICO (2007) *Annual Report 2006 – 07*, p. 24.

[118]. Overall, prosecutions are thus clearly initiated in only a minute fraction of all cases in which there was a criminal breach of the *Data Protection Act 1998*. In the vast majority of cases, the ICO seeks to resolve situations - even situations in which there is a clear breach of the Act - by discussions and negotiations with the relevant controller. This is successful in the sense that, in those cases, an end-result is reached which, at least in the view of the ICO, is compatible with the DPA98 (or at least acceptable to the ICO, who does not like to take too literal or legalistic a view of these matters, and prefers to just make sure that the right balance is struck, as he sees it). This may be less acceptable to any data subject who happened to raise the issue, and is likely to have been at the centre of the case at the beginning. But it is unfortunately the case that these individuals tend to get somewhat 'lost' in the negotiations between the ICO and the controller: they are certainly not usually invited to directly participate in them, although at times (as with the City Council) they may obtain the relief they sought. This is further discussed in section 4.2 below.

[119]. A more general problem is that the ICO's approach may give the impression of 'soft' and negotiable enforcement of the law, which is not conducive to wider compliance and may in part account for the widespread disregard for even the most basic requirement of the Act, notification of processing operations. This problem is not unique to the UK - similar criticism is voiced in other EU Member States. But it contributes to the overall weakness of data protection in the UK legal order, already encouraged by the weak constitutional/legal basis it has in the country (as discussed in section 1.1, above).

[120]. In addition, there is a question of transparency and fairness. The ICO's Annual Reports give a few selected examples of how the negotiations between the ICO and certain controllers led to certain data subjects' problems being resolved. But they give little or no insight into the underlying principles or compromises, even in these selected cases. We know nothing of the vast majority of the 13,400 cases 'resolved' by 'advice' and 'negotiation'. Presumably - indeed, inescapably - some of these cases must have thrown up basic questions, such as whether certain data constituted 'personal data' (cf. the *Durant*[95] case), or whether a certain secondary use of certain data was or was not 'compatible' with the primary use for which they data had been obtained, and/or whether the data subject should have been (or still should be) informed of this and given a chance to object, or for how long it was 'necessary' to retain the data, or whether certain measures adequately anonymised or pseudonymised the data, etc…It is in these kinds of cases that the law is made. Yet we know almost nothing of them. As further discussed in section 2.5, the 'negotiable' approach to data protection, adopted by the ICO, thus means first of all that justice is not seen to be done - which is contrary to the Rule of Law, and feeds suspicions that big companies and organisations can negotiate arrangements that are not in accordance with the Act as others than the ICO would read it - or with the Directive or the ECHR, which the ICO doesn't take into account in any case.

[95] *Durant v Financial Services Authority* [2003] EWCA Civ 1746.

What is more, it means that the law is not openly developed, in a way that allows for public debate and criticism. This too is not healthy.

2.2.8. Analysis of whether the ICO's resources are sufficient to ensure the effective use of his powers

[121]. In the previous section, it was noted that the enforcement practice of the ICO is quite 'soft', and that many issues - and violations of the law - are not seriously investigated or pursued through enforcement action. One question that arises is whether this is the result of a lack of resources, and/or the way they are used (or perhaps must be used under the law).

[122]. It must be stated first of all that there is no reason to doubt that, within the terms of its own and Government policies, the ICO appears to be run to broadly acceptable standards - although some of the comments ('broadly adequate', 'generally...satisfactorily', 'keen to improve') suggest that there is room for improvement in specific areas. To quote the ICO's own *Statement of Internal Control* for the last year:

'The internal auditors have a direct line of communication to me [i.e., the ICO - DK] as the Accounting Officer. In addition the internal auditors regularly report to the Audit Committee in accordance with government internal audit standards, including their independent opinion on the adequacy and effectiveness of the ICO's system of internal control. The internal auditors also provide an annual statement which expressed the view that, in the areas they scrutinised this year, established procedures were broadly adequate to meet management's overall objectives, and that controls were generally operating satisfactorily with those areas of potential improvement highlighted. It is especially reassuring that the internal auditors were able to conclude that the ICO was well managed, keen to improve and took account of audit recommendations.'[96]

[123]. Beyond this, it should be noted that, although it provides all of the funding for the ICO's data protection work (as noted in section 2.1 above), notification must also use up a seizable part of the ICO's human and other resources. There are no specific figures on this in the ICO's Annual Reports or in the Accounts that are attached to each of them. Indeed, the latest report does not even mention how many new or renewal notification cases were dealt with in the year concerned, other than how many there were (287,000 in 2006-07). In the previous year, somewhat more detailed figures were provided, as follows:

'We received nearly 36,000 new notifications in 2005-2006, this was around 5,000 fewer than the previous year. Renewals processed for 2005-2006 numbered 240,000, almost 15,000 more than the previous year. The total

[96] ICO(2007) *Annual Report 2006/07,* p.72.

number of changes processed for 2005-2006 was 69,000, an increase of almost 14,000.'[97]

[124]. All this work is done in spite of the fact that it has been felt by many people, for many years, that notification serves few sensible purposes, and is largely a waste of resources. As the author of the present report already concluded in 1997, also on the basis of the views of the European (and UK) data protection authorities:

'Comprehensive registration of processing operations...serves little purpose, is bureaucratic and impractical, and unenforceable (and not effectively adhered to or enforced) in practice.'[98]

[125]. This is of course not the fault of the ICO, who is both required to receive and process notifications (and indeed to force controllers to notify their operations), and dependent on the fees they bring in for his data protection work. But in a broader context it is still a matter that should be addressed.

[126]. Whether, after managing notifications, giving advice and guidance, reporting to Parliament, expressing concerns, consulting and studying, cooperating with other Data Protection Authorities, and informing the public, there are sufficient resources left for (real, hard) enforcement, is a moot question: it depends on one's priorities, indeed on the view of the office of the Commissioner. The current Commissioner clearly and explicitly sees his role as mainly an advisory, 'helpful hand' one - and not as a fierce guardian of a fundamental human right. He therefore puts most of his resources into relatively gentle 'guidance' and 'expressions of concern' and statements urging the authorities (and others, in the private sector) to carefully balance the interests - without very often trying to impose his views of what the law (the DPA98) demands. He explicitly refuses to even examine what the *European Convention on Human Rights* or the EC Directives demand. His resources are probably sufficient for this limited, 'soft' role. But if the aim were to be to truly and forcibly enforce the Act - and the European standards - they are manifestly lacking.

2.3. Remit

[127]. As noted, the remit of the Information Commissioner extends to both the *Data Protection Act 1998* (DPA98)[99] and the *Freedom of Information Act 2000*[100]

[97] ICO (2006) *Annual Report 2005/06*, p.30, available at: http://www.ico.gov.uk/upload/documents/library/corporate/detailed_specialist_guides/annual_report_2005.pdf (26.01.2009).

[98] D. Korff (1997) *EC Study on Existing Case-Law on Compliance with Data Protection Laws and Principles in the Member States of the European Union, Final Report*, p. 63. Emphasis omitted.

(FOIA). The ICO is also responsible for international cooperation, in the WP29 group and in other European fora (Europol, Eurojust, etc.) and world-wide. It may be useful to add a few comments about the substantive scope of the DPA98, about the exemptions from all or part of the Act, and about the vexed issue of territorial scope, because the ICO can of course only be active in, and use its powers in relation to, matters that are covered by the Act.[101]

[128]. Because of the rather peculiar way in which the DPA98 transposes the definitions from Directive 95/46/EC into domestic law, the definition of its scope is also somewhat odd. Thus, the Act says (in s.6(1)) that it applies to '[any] data controller in respect of data' (rather than to 'processing of personal data…by automated means, and to the processing…of [manual] personal data which form part of or are intended to form part of a [structured] filing system,' as it is put in the Directive), but by defining 'data' as information that is either automatically processed or part of a 'relevant [i.e., structured] filing system,' this effectively comes down to the same thing.[102]

[129]. The Act does not extend to 'legal persons' (such as companies or associations) or deceased persons (because data on either of these fall outside the definition of 'personal data'). However, the *Privacy and Electronic Communications (EC Directive) Regulations 2003*,[103] in giving effect to the *e-Privacy Directive*, do extend some rights to legal persons.

[130]. The Act is not limited to matters within the scope of EC law, but in principle applies to all controllers who process personal data, subject to some broad exemptions and derogations in respect of certain controllers or processing operations, and to the 'applicable law' provision, briefly mentioned below.

[131]. On the first issue, the Act contains a number of broadly-phrased exemptions concerning national security, prevention or detection of crime, tax, etc. (ss. 28 and 29). Another broad exemption (further regulated in certain Regulations) applies to data and processing concerning health, education and social work (s.30). The Act also (in accordance with the Directive) contains a general

99 UK/Data Protection Act c.29 (16.07.1998), available at: http://www.opsi.gov.uk/Acts/Acts1998/ukpga_19980029_en_1 (26.01.2009).

100 UK/Freedom of Information Act 2000 c.36 (30.11.2000), available at: http://www.opsi.gov.uk/Acts/acts2000/ukpga_20000036_en_1 (26.01.2009).

101 The following paragraphs are largely taken from the 'Country Report on the UK', issued on CD-ROM with D. Korff (2006) *Data Protection Law in Practice in the EU*, Brussels/New York.

102 The Act also includes in the definition of 'data', information that forms part of what it calls an 'accessible record.' The latter is separately defined in section 68: it refers to certain health and educational records and a long list of "accessible public records" set out in a separate schedule to the Act (Schedule 12). In effect, in this rather cumbersome way, the Act thereby extends its scope to manual records of the kinds mentioned, irrespective of whether they are 'structured' or not.

103 UK/The Privacy and Electronic Communications (EC Directive) Regulations 2003 SI 2426 (11.12.2003), available at: http://www.opsi.gov.uk/si/si2003/20032426.htm (26.01.2009).

exemption concerning 'personal data processed by an individual for the purposes of that individual's personal, family or household affairs (including recreational purposes)' (s.36). A complex, qualified exemption furthermore applies for 'journalistic, artistic and literary purposes' (s.32); and another qualified exemption relates to processing for research purposes (including 'statistical or historical purposes').

[132]. The Act tries to faithfully implement the 'applicable law' provision (Article 4) of the Directive, but the ambiguities of the European rules also make the British statutory provisions difficult to apply. Thus, the Act provides, first of all, that the Act applies to a data controller 'in respect of any data' 'if the controller is established in the United Kingdom and the data are processed in the context of that establishment' (s.5(1)(a)).[104] The crucial issue is thus the place of establishment of the establishment (e.g., branch) in the context of whose activities the processing takes place, at least when that place is within the EU/EEA. If a controller is not established in the UK or in any other EU/EEA State, the UK Act applies if that controller uses equipment in the UK for the processing of the data (unless the data merely pass through the UK in transit) (s. 5(1)(b)). This is basically also as the Directive requires.[105]

[133]. If the UK DPA98 does not apply, but processing is subject to the data protection law of another EU/EEA State, the ICO may, under the EC Directive, be called upon to assist the Data Protection Authority of that other State in the application and enforcement of that other law - but this rarely happens, if ever; there are no examples of it having happened in the Annual Reports.

2.4. Independence

[134]. Unlike in some other Member States, where the Data Protection Authority (DPA) is appointed by Parliament, the UK Information Commissioner is appointed by the Government (in formal terms, 'by Her Majesty [the Queen] by Letters Patent': s.6(2) DPA98). Although, as discussed in section 2.2.3.4, he does report to Parliament both annually and ad hoc, he is neither a creature of Parliament nor responsible to it, and he cannot be dismissed by it. The arrangements under which he operates have varied, as a result of changes in the structure, departments and ministries of Government. Originally, responsibility for what was then called the Data Protection Registrar was vested in the Home Office (the UK equivalent of a Ministry of Interior Affairs). In 2001, it passed to the Lord Chancellor's Department, and in 2003, to the newly created Department for Constitutional Affairs, which was replaced by the Ministry of

[104] The Directive refers to processing which is carried out 'in the context of *the activities of* an establishment of the controller' but the difference would appear to be merely semantic.

[105] For a somewhat more detailed discussion, see 'Country Report on the UK', issued on CD-ROM with D. Korff (2006) *Data Protection Law in Practice in the EU*, Brussels/New York.

Justice in 2007 - and that is where it still is.[106] Or to put it in current Whitehall terminology, the Information Commissioner is now 'sponsored' by the Ministry.[107]

[135]. As explained in para.57 above, the way in which the ICO will carry out his functions and can spend the fees paid for notification (registration) by controllers - which is the only source of funding for his data protection work - is governed by a *Framework Document* and a *Financial Memorandum* concluded between the ICO and the Ministry (for the year 2006/07, still between the ICO and the Department for Constitutional Affairs). As also explained there, these contain, *inter alia*, rules and guidelines on how the Commissioner shall exercise his functions, duties and powers, arrangements on his use of public money (that is, for data protection work, of the fees collected through notification), and the relationship between the Commissioner and the Ministry generally.

[136]. The above means that the ICO is quite tightly controlled by the Government: it appoints him (or her) and holds the purse-strings (it is the Government that sets the notification fee, and it has not increased this for years), and considerably ties him down through these negotiated Framework Documents and Financial Memoranda. In practice, much will depend on the character and personality of the Commissioner him- or herself. There is no doubt that the current incumbent feels quite free to speak on relevant issues, and he has taken some very forceful stands on freedom of information issues (especially on access to information relating to the Iraq war) - although, as discussed, he is much 'softer' on data protection matters. But it is still doubtful whether his office can be said to fulfil the requirements set out in Article 28(1) of the Directive, which stipulates that Member States must establish national supervisory authorities of such a kind that it is ensured that they 'shall act with complete independence in exercising the functions entrusted to them.'

2.5. Role of the Opinions of the Working Party established under Art. 29 of Directive 95/46/EC

[137]. The WP29 opinions are definitely not considered binding in the UK. They are sometimes referred to by the ICO, but not often, and always as little more than informal guidance. There is little evidence that they are used by the ICO as direct inspiration for its own views on how the UK DPA98 should be applied. Indeed, more often it is civil society groups that are referring to them and urging the ICO to apply the UK Data Protection Act in accordance with the WP29 opinions, but with limited success.

[106] ICO (2007) *Annual Report 2006/07*, p. 60 (in the Foreword to the Accounts).
[107] ICO (2007) *Annual Report 2006/07*, p. 60 (in the Foreword to the Accounts).

[138]. Other WP29 documents are given even less status. Thus, e.g., the UK Government's plans for secondary research and other uses of NHS patient data are clearly contrary to the Directive and the guidance given on Electronic Health Records in WP document no. 131, but the Government ignores this and the ICO is not demanding that the WP views are followed.

[139]. The WP29 opinions and documents are not made available to the public on the data protection part of the ICO 'Document Library', even though the introduction page says that the library is 'a comprehensive resource for individuals and organisations' that contains 'all the documents you'll need to keep informed and up to date.'[108]

[140]. On the 'Links and Resources' webpage, there is a general link to the European Commission's data protection page, from where one can click through to the WP29 pages, but there is no direct link to the WP29 pages or resources.[109]

2.6. Public Information and –awareness

[141]. The ICO *Annual Report 2006-07* the following overview of the ICO's public information and awareness activities:

'The highlight of the year was launching our new website www.ico.gov.uk in August 2006. In response to user feedback, we produced material aimed more specifically at individuals or organisations, improved the navigation and provided more information about the ICO. The new site allows people to find out about data protection and freedom of information matters as they occur in real life, by following links on topics such as credit, health, housing, education and junk mail. Similarly, people with data protection and freedom of information responsibilities at work are able to follow links on the most frequent areas of need, such as employment, setting up a new business, and marketing.

This year also saw the start of a new programme of publications, designed to fill gaps in the information we provide, and to offer the right level of information for users' needs. Highlights for data controllers include a new training DVD, 'The lights are on', to help people get data protection right in the workplace, as well as a new guide to notification. For individuals, the ICO launched a 'Personal information toolkit' in January, to mark European Data Protection

[108] See: http://www.ico.gov.uk/tools_and_resources/document_library/data_protection.aspx (21.03.2009).

[109] See: http://www.ico.gov.uk/tools_and_resources/links_and_resources.aspx (21.03.2009). (The link for the European Commission under 'E' leads to: http://ec.europa.eu/justice_home/fsj/privacy/)

Day. The booklet was designed to help people protect their personal information, and was promoted by a set of public information adverts. We also launched a new series of consumer fact sheets called 'It's your information', which focus on data protection matters in everyday situations. This is a stablemate for the now established Good Practice Notes we produce for data controllers, which continue to attract the attention of trade and specialist media.

We distributed over 306,000 publications altogether, a rise of about 38% over last year. Our most popular leaflet remains 'Credit explained', a consumer guide to personal information and credit (we sent out over 72,000 copies). 'Your guide to openness', our guide to freedom of information, remained in the top five most requested publications, with around 40,000 being distributed. In response to customer requests for more information about the ICO, we launched a quarterly e-newsletter, as well as two leaflets on what the ICO does and the legislation we cover.

Wide-reaching media coverage of data protection and freedom of information stories demonstrates a high level of public interest in the issues. Freedom of information and environmental information decision notices continued to provide a steady source of media stories covering topics as broad as empty council properties, ministerial advice on salmon fishing, MPs' expenses and aircraft noise. Our international data protection conference in London in November, which focused on the topic of the Surveillance Society, gave rise to significant national and international media coverage. Overall, the ICO generated over 1,500 media items in 2006/07 reaching a combined audience of over 356 million.'[110]

[142]. The above is undoubtedly an impressive effort, and there is now clearly widespread awareness amongst the public and data managing professionals of the existence of the DPA98 and data protection generally, and of specific rights and duties under the Act (as further discussed in section 5 below). The information made publicly available by the ICO is clearly sufficient for that purpose: awareness-raising.

[143]. However, one can be more critical about the extent to which the information produced by the ICO suffices to give clear and precise guidance on the law, or a real insight into his work and priorities.

[144]. The first matter that should be noted is that the full legal texts relevant to data protection in the UK are not all directly available, in easily accessible and downloadable format, from the ICO website. Even the main law, the DPA98, cannot be simply downloaded in full, in word or pdf format - which is in contrast to the websites of almost all other EU Data Protection Authorities, from which the national laws (and often all regulations, and even translations into English, can be readily obtained in this way). This is partly because the UK

[110] ICO (2007) *Annual Report 2006-07*, pp. 47 – 48.

Government generally does not allow the downloading of entire laws, in one document: instead, Government departments, and bodies such as the ICO, are only allowed to provide a link to the body that published the laws, OPSI. Through the link on the ICO website, one can access the DPA, but only page-by-page; the full Act cannot simply be downloaded in its entirety by one 'click'.[111]

[145]. The website also does not contain a clear collection of all relevant legal texts. The visitor is directed to a link of which the website says, under the heading 'data protection': 'Need to know more about the law and your personal data? All the information's here and more...'. In fact, if one follows that link, one is directed to a page that provides further links, to large amounts of 'practice notes' and guidance and forms, all explaining what the law requires and how it should be applied (in the opinion of the Information Commissioner), but which do not include any links to the actual legal texts.[112] There is similarly no simple collection on the ICO website of all relevant laws, regulations, legal decisions and rulings by the courts. This makes it not just difficult for academics to study the operation of the ICO, and the application of the law - more importantly, it hampers critical monitoring of the ICO and the operation of the law by citizens and NGOs.

[146]. A further serious matter is that there is little or no insight - other than through examples which the ICO chooses to highlight in its reports, without clarifying why those were chosen - of the outcome of the ICO's 'negotiations' with controllers. This lack of transparency means that there will be doubt as to the equal application and enforcement of the law (it would seem for instance quite telling that many major companies appear to have signed 'undertakings' with the ICO, promising to behave in future, while most prosecutions have been against small companies and individuals). This lack of clarity of how the law is interpreted and applied in practice also has implications at the European level, in that it leaves somewhat unclear whether the EC directives are properly implemented in the UK.

[147]. Furthermore, as already noted, the ICO's Annual Reports are also not as revealing in terms of statistics as could be hoped for: cf. the confusing categories of cases and figures in the Chart in para.103, and the comments in

[111] Click on the hyperlink 'Data Protection Act 1998' on the following page: http://www.ico.gov.uk/what_we_cover/data_protection/legislation_in_full.aspx (26.01.2009). This leads to the following page, of the Office of Public Sector Information (OPSI): http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1 (26.01.2009). As it is said on that page, 'OPSI encourages users to establish hypertext links to this site' - but it is not a user-friendly format.

[112] The first page is: http://www.ico.gov.uk/tools_and_resources/document_library.aspx (26.01.2009). If one follows the link mentioned in the text, one is directed to: http://www.ico.gov.uk/tools_and_resources/document_library/data_protection.aspx . But there are no links on that page to the actual text of the DPA98, or of the other basic legal instruments on data protection. A list of all the guidance and notes, etc, is provided separately with this report.

the paragraphs after that, noting that it is impossible to see from the statistics in how many cases possible or probable breaches of the law were not pursued because they did not reached the 'assessment criteria' (which themselves are not easy to find). Nor is it clear what proportion of the ICO's budget is spent on notification (para.123, above).

[148]. Much of this information could possibly be obtained through freedom of information requests - but it would be ironic if that were to be the only way in which clear transparency could be achieved with regard to the FOI Act's own watchdog. It would be much better if the ICO made much more basic information accessible, in full, in easily downloadable format. His guidance and interpretation help is all very well - but not everyone will always agree on his reading of the law. The question of 'soft' and seemingly negotiable application of the law, and the availability of full information over how the law is applied in all instances are clearly linked. Until there is full transparency, there will be doubts about the fair and equal and full application of the law by the ICO.

3. Compliance

[149]. As noted in section 2.2.7 in particular, compliance with the DPA98 is not very high, if one judges this by the number of registered controllers, which is only a fraction of the number one would expect if there were to be full compliance (less than 300,000 registered controllers in the UK overall, in contrast to some 2.300,000 registered companies in Great Britain alone, without counting individuals that may need to register). With enforcement being 'soft' and focussing on 'low-hanging fruit' (as extensively discussed in section 2.2.7), it must also be assumed that compliance in other areas is also low.

3.1. Appointment of data protection officers

[150]. The UK DPA98 does not require that companies or government bodies appoint an in-house data protection- (or information-) officer or –official. The ICO will undoubtedly see it as a positive step if a company or public body appoints such an official, but this is not required or indeed specifically encouraged. Thus, for instance, in the FAQs answered on the ICO website, such an appointment is not mentioned (even as an optional, non-mandatory but encouraged possibility) under the question: 'What do I need to do under the Data Protection Act?'.[113]

[151]. Even so, in practice, many organisations do appoint such an official. The consultancy and seminar-organisation firm 'Privacy Laws & Business', which is based in the UK, is host to the European Privacy Officers Network (EPON), which has many UK members.[114] However, this is a purely private initiative, without any formal input from the ICO (although staff members from the ICO may from time to time address this forum).

[113] See: http://www.ico.gov.uk/Global/faqs/data_protection_for_organisations.aspx (21.03.2009).
[114] See: http://www.privacylaws.com/templates/Events.aspx?id=364 (21.03.2009).

4. Sanctions, Compensation and Legal Consequences

4.1. Criminal Sanctions

[152]. Criminal sanctions and prosecutions have been discussed in section 2.2.7, above; a list of the offences created by the DPA98 is provided separately. Suffice it to recall here that prosecutions are initiated in only a minute fraction of all cases in which there was a criminal breach of the Act (in particular, failure to notify [register]), and that in the vast majority of cases, the ICO seeks to resolve situations - even situations in which there is a clear breach of the Act - by discussions and negotiations with the relevant controller. See paras.99ff, above.

4.2. Investigation of complaints

[153]. As noted in para.98, above, the ICO does not go out of his way to try and uncover breaches of the Act unless they somehow become exposed. If an individual complains of an alleged breach of the law by a controller, the complainant is first told to try and resolve the issue with that controller, and in particular to first use any remedy or complaints procedure which the controller may have established, which may take quite a bit of time and effort on the part of the data subject. So it will be only quite persistent complainants whose cases are actually even properly registered. Yet as we have seen, this still amounted to some 24,000 cases in the year 2006-07.

[154]. The handling of these cases has already been discussed in section 2.2.7, at para. 101ff, above. It will suffice to recall here that:

- most cases (13,400) were dealt with 'simply' through 'advice and guidance' (even though some of these cases were 'extremely complex');[115]
- more than a third of the remaining 10,000+ cases were not actually assessed with a view to determining whether the law had been broken, because they did not meet the 'assessment criteria' (set out in para.104, above); and
- the ICO found that it was 'likely' that a breach of the law had occurred in 3,600 of the remaining 6,500 or so cases.

[115] ICO (2007) *Annual Report 2006/07,* p.12.

[155]. Oddly, the Annual Reports do not actually reveal, even in broad terms, how those 'likely' breaches of the DPA98 were ultimately dealt with. All we know is that the ICO obtained some 36 formal 'undertakings' from companies and public bodies, under which they promised to behave in future;[116] that 25 Enforcement Notices were issued since December 2006, of which there were 6 in the year 2006-07;[117] and that there were 14 prosecutions in that year (and similar numbers in previous years).[118] The *Annual Report 2006-07* does make clear that several cases, against one or a few companies or organisations, arose out of 'many' or 'hundreds' of complaints, but it seems likely that the cases involving undertakings, enforcement notices or prosecutions still only constitute a small proportion of the 3,600 cases in which a violation of the law probably occurred. Presumably, all the cases (of this total) that did not involve undertakings, enforcement notices or prosecutions were resolved in other ways, to the satisfaction of the ICO.

[156]. Whether the resolution in those cases was also to the satisfaction of the complainants is more difficult to tell. The ICO's Annual Reports do contain statistics on the satisfaction levels of the ICO's 'customers', but these are not broken down in relation to issues dealt with.[119] It would have been useful to know what percentage of complainants was happy to learn that their case would not even be assessed because it did not meet the 'assessment criteria', or that the ICO, after assessment, had decided that it was 'unlikely' that a breach of the Act had occurred.

[157]. As concerns the 3,600 cases in which the ICO held that a breach of the Act had been 'likely' (most of which will have come to the attention of the ICO as a result of complaints), it would similarly have been useful to know whether the individuals concerned were happy with that resolution. The impression one gets is that individual complainants are not involved in the process leading to the resolution, and that they are not asked if they are satisfied with the resolution (either before or after it is formalised); cf. the following passage in the main guide issued by the ICO to potential complainants:[120]

---

[116] The notices and formal 'undertakings' are listed on two pages in the ICO 'document library'. See: http://www.ico.gov.uk/tools_and_resources/document_library/data_protection.aspx#notices; http://www.ico.gov.uk/tools_and_resources/document_library/privacy_and_electronic_communications.aspx (26.01.2009).

[117] See para. 111 above.

[118] See the Chart in ICO (2007) *Annual Report 2006/07*, pp. 56-57 (but see footnote 93). For discussion, see para. 115ff., above.

[119] The ICO was given the following ratings by individuals: Excellent: 14%; Very good: 22%; Good: 20%; Fair: 12%; Poor: 28%; Don't know: 3% (for controllers, by the way, the figures were 9, 23, 34, 20, 15 and 0%, respectively). See ICO (2007) *Annual Report 2006/07*, p. 16. Note that the sample base was very small: just 202 individuals (and 128 controllers).

[120] ICO, *The Data Protection Act 1998 – When and how to complain*, p. 8, available at: http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/dp_how_to_complain_final.pdf (26.01.2009).

'If we decide to look into your complaint, we will usually contact the organisation concerned. This may lead to an outcome we regard as satisfactory, and if so we will let you know what has happened.'

[158]. It is unclear how detailed the information is that is provided to a complainant at the end of this process; there is no information as to what percentage of complainants were contend with it. The last sentence also suggests that complainants are not informed if the ICO cannot achieve a satisfactory outcome (and perhaps may therefore resort to prosecution), but this may not be intended, and complainants are perhaps also informed in such cases.

[159]. Of course, under the Act, individual complainants also have no possibility to challenge the outcome. In particular, unlike controllers, individual complainants cannot appeal to the *Information Tribunal*. They can, in theory, apply for judicial review of the ICO's decisions and actions, but that is a costly and time-consuming remedy, with uncertain outcome and of limited scope, in that the actions of the ICO would only be subject to marginal review. It is not realistic to expect individuals to use this remedy other than in exceptional circumstances (or if the individual was very rich).

[160]. Overall, the status of people who claim to be victims of violations of the DPA98 is therefore weak, and not much strengthened by the ICO. The Office will help individuals who it deems to have a meritorious case (especially if there are many of them and there is evidence of a widespread problem), and it will seek on their behalf an 'acceptable' solution to their problems, based on its (the ICO's) views of what strikes a reasonable balance between the interests of the complainants and those of the controllers. It will not give much support to individuals who seek a strict, uncompromising application of the law, or who disagree with the ICO on a particular interpretation of a particular term in the Act (or who argue that an issue arises in relation to one of the EC directives or the ECHR).

4.3. Compensation

[161]. As the ICO explains:

'**We have no powers to award compensation**. If you have suffered a loss because an organisation has broken the law, you may be entitled to compensation. You must claim this through the courts.

The right to compensation applies even if you don't report the problem to us. You can make a claim to the court whether or not we have agreed that the law has been broken.'[121]

[162]. The ICO has also issued a more detailed guide on this. It may suffice to quote the basic outline of the situation from that guide, as follows:

'When can I claim compensation under the Act?

You have a right to claim compensation from an organisation if you have suffered damage because they have broken part of the Act.

You can normally only claim for any distress you have suffered if you have also suffered damage. However, if the organisation broke the Act when they used your information for journalism, artistic or literary purposes, you can claim for distress alone.

How do I make a claim for compensation?

You do not have to make a claim to a court if an organisation agrees to pay you compensation. If you cannot reach an agreement with them, you can apply to a court for compensation alone or you can combine your claim with an action to put right any breach of the Act.

The Information Commissioner cannot award compensation, even when he has said that in his view the organisation did break the Act. You would still have to make a claim to a court.

Will it help me in court to have asked the Information Commissioner whether the Act has been broken?

It may do. You can ask the Commissioner to assess if the organisation broke the Act and he will tell you whether, in his view, it was likely or unlikely that the organisation broke the law. You can give a copy of his letter to the court together with the evidence you have to prove your claim. However, a court will take their own view of the law and the judge may well not agree with the Commissioner's view.

You may wish to ask our helpline first to see if it is worth asking the Commissioner to assess your complaint. You can find a complaints form on our website. Whether you complain to the Commissioner or take a case to court, you will need evidence to back up what you say.

---

[121] ICO, *The Data Protection Act 1998 – When and how to complain*, p. 11, available at: http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/dp_how_to_complain_final.pdf (26.01.2009). Original emphasis in bold.

How much will the court award me if my claim is successful?

There are no guidelines about levels of compensation for a claim under the Act. It will be up to the judge hearing the case and he would take into account all the circumstances, including how serious he thought the breach was, the impact it had on you, particularly when assessing the distress you suffered. Even when you can show the court the exact sum of money you have lost as a result of the breach of the Act, it is still up to the judge to make the award and he may reduce your claim or award nothing at all.

It is also important to remember that even if the court awards you compensation, the organisation may refuse, or not be able to pay. If this happens you should ask the court about what you should do to enforce the judgment.'[122]

[163]. The ICO has issued yet a further leaflet in this respect, which sets out the legal details.[123]

[164]. One problem with the court system is, of course, that it can expose a claimant to liability for the legal costs of the other party. As the ICO points out in the latter leaflet, it is unlikely that a court will order a claimant to pay damages in a minor 'small claims' procedure, but if major issues or claims are at stake, this is a very significant risk.

4.4. Enforcement of data protection legislation, information and assistance of data subjects, legal assistance and representation

[165]. As noted, the ICO's Annual Reports contain information and statistics on the actions taken by the ICO on cases brought to its attention: see section 2.2.7, para.88ff, more in particular paras. 100 – 120 and the Chart in para. 103. As noted, some 24,000 cases come to the attention of the ICO each year, of which approx. 13,000 are dealt with through simple advice.

[122] ICO (2006) *Claiming Compensation*, p.11-12, available at: http://www.ico.gov.uk/upload/documents/library/data_protection/introductory/claiming_compensation_2.0.pdf (26.01.2009).

[123] ICO, *Data Protection Act – Taking a Case to Court*, undated, available at: http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/taking_a_case_to_court.pdf (26.01.2009).

[166]. The Annual Reports do not clarify how many of these queries come from organisations (enquiring perhaps about how to register, or how to handle data subject access requests), and how many from data subjects (presumably complaining or at least asking about their rights). However, it may be assumed that at least the cases that were seriously assessed in order to ascertain whether there had been a breach of the DPA98 mostly derived from complaints brought by data subjects (or perhaps by organisations representing them). As shown in the Chart in para. 103 above, these amounted to 6,500 cases in 2006-07, broken down as follows (the percentages below are in relation to the total number of 24,000; relative to each other the figures are 12/27= +45% and 15/27= +55%):

12 %	± 2,900	Cases that were considered on the merits and in which it was concluded that it was "unlikely" that a breach of the Act had occurred
15 %	± 3,600	Cases that were considered on the merits and in which it was concluded that it was "likely" that a breach of the Act had occurred

[167]. With respect to the question, whether data subjects are sufficiently informed and assisted by the data protection authority, one should distinguish. The ICO undoubtedly provides extensive general advice on the DPA98, also to data subjects; there are many leaflets and guides available from the website or otherwise.[124]

[168]. Data subjects are also generally well informed if they contact the ICO, e.g. through the helpline, the telephone numbers for which (08456 30 60 60 or 01625 545 745) are given at: http://www.ico.gov.uk/complaints.aspx .

[169]. One can be more doubtful as to whether data subjects are sufficiently assisted by the ICO if they want to take their case further. As noted, the ICO sees its tasks mainly as conciliatory; it tries to reach a solution which it finds acceptable, without seriously involving the data subject/complainant in this. It is rare for the ICO to take strong enforcement action in support of single individuals; it tends to reserve such action for wider problems, affecting large numbers of people or raising serious issues of principle.

[170]. The position of individuals is all the more invidious in that they are not entitled to legal aid (free legal advice and assistance in court) in any cases they may wish to take. The only actions open to individuals are proceedings in the civil courts, which are very expensive. In practice, only rich individuals or people backed by NGOs can afford to really mount a serious legal challenge in the

[124] See: http://www.ico.gov.uk/tools_and_resources/document_library/data_protection.aspx (21.03.2009).

courts against practices they regard as contrary to the DPA - and it would be even more difficult to mount an action on the basis that the Act fails to properly implement the Directive (even though, in theory, under EC law, individuals who suffer harm as a result of a failure to implement a directive should be able to sue). Even most NGOs cannot afford to support such cases. The above is one of the main reasons why, in the UK, there is so little clear case-law on data protection issues. (As noted, organisations can appeal to the Information Tribunal from a ruling by the ICO with which they disagree, but this remedy is not available to data subjects).

4.5. Protection of personal data in the context of employment

[171]. The ICO has given considerable attention to the application of data protection law in an employment context, but most of its advice is aimed at employers (although, presumably, if it is followed it will also assist employees, and employee/data subjects and their legal and trade union advisers can of course draw on this guidance too). The main webpage for this is: http://www.ico.gov.uk/for_organisations/topic_specific_guides/employment.aspx (21.03.2009).

[172]. This page (and other pages, e.g. in the 'Document Library') provide links to a range of documents on the matter, including a major 'Employment Practices Code', with subsequent 'Supplementary Guidance' and a 'Quick Guide'. The Code (and the Supplementary Guidance) is not legally binding but, as it says in the Introduction, compliance with the Code will 'protect organisations from legal action – adhering to the Code will help employers to protect themselves from challenges against their data protection practices.'[125]

4.5.1. Role of Work Councils and Trade Unions

[173]. Works councils are not common in the UK (although there are occasional calls to introduce them); to quote from a website on such councils throughout the EU:

[174]. 'In contrast to other EU member states, works councils are rare in the UK. At best, employers may have a staff consultation committee or forum, which is usually a fairly low-key conduit for management passing information to the workforce about the business's performance with some feedback and questions

[125] ICO (2005) *Employment Practices Code*, p.3 and 4, available at: http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/employment_practices_code.pdf (21.03.2009).

from attendees. Employees are only normally collectively represented through trade union recognition or where statute requires employee consultation, most notably in relation to collective redundancies and transfers of undertakings. Crucially, no consultative body has the power to block or even delay any actions of the employer, albeit there may be financial penalties to reflect failures to comply with specific statutory requirements. (...)'[126]

[175]. Trade unions also play only a very limited role in data protection matters; many are not well versed in the matter. In most organisations (public or private) there is little employee awareness of, or involvement in discussions on, data protection in the employment context. The WP29 opinions and documents on the issue are largely unknown, even to employee organisations.

[176]. Of course, if there is a specific, serious dispute between an employee and his or her employer, especially if the employee is a trade union member, a union will support the individual, also with legal advice and counsel. But data protection is not an issue that is brought up very often by trade unions more generally, or indeed one on which they provide much advice.

For instance, a quick search of the website of the main trade union for academics, the UCU, using the search term 'data protection', brought up a long list of documents, but only a few of them seemed to be particularly concerned with data protection. One document that seemed particularly relevant, the 'UCU advice on disclosure of job evaluation data', contained a section on data protection that was very short, flimsy and seemingly out of date (it was also undated, and in some respects seems to be based on the previous rather than the current Act).[127]

[126] Wragge & Co: *European Employment Law Checkpoint* , available at: http://www.wragge.com/eelc_3504.asp (21.03.2009).

[127] See: http://www.ucu.org.uk/media/pdf/r/i/ucu_disclosurejedata.pdf (21.03.2009).

5. Rights Awareness

[177]. As noted in section 2.5 above, the ICO is active and effective in raising awareness of data protection law and the rights and obligations it creates. As it says in its *Annual Report 2006/07* (in a passage also covering freedom of information awareness):

'Efforts to improve our communications are paying off. More people are now aware of their data protection rights (82% of individuals compared to 76% last year). Awareness of freedom of information rights among individuals remains high at 73%. Awareness among practitioners is very high: 94% are aware of data protection rights (compared to 91% last year) and 97% are aware of freedom of information rights.'[128]

[178]. As already noted, the ICO leaflets and guides etc. on these issues are helpful and easy to understand.

6. Analysis of deficiencies

[179]. The deficiencies in the UK regime have already been noted. Briefly:

- data protection has a weak constitutional basis;
- the courts are disinclined to give strong protection to personal information and privacy;
- the DPA98 fails to properly implement Directive 95/46/EC, and many matters are regulated not through binding law but by means of non-binding guidance;
- the UK Data Protection Authority, the ICO, is quite tightly controlled by Government; it is doubtful whether the ICO has a sufficiently independent status in terms of the Directive;
- the ICO does not apply EC law or ECHR principles in his enforcement of the DPA98;
- its enforcement of the DPA98 is generally 'soft' and aimed at reaching 'negotiated resolutions' to issues, rather than at strict application of the law; tougher enforcement measures such as the imposition of Enforcement Notices or prosecutions are reserved for a very few, easy-to-prove cases of manifest abuse;

[128] See: ICO (2007) *Annual Report 2006/07*, p. 47-48.

- the details of the 'negotiated resolutions' reached in the vast majority of cases are not made public and the application of the law is therefore not transparent;
- it is difficult for individuals to assert their rights: the ICO provides only limited support to them (again, aimed mainly at reaching 'negotiated resolutions', without involving the individuals in the negotiations); for 'harder' enforcement, or to obtain compensation, they must go to court, which is expensive and time-consuming;
- compliance with the law is (unsurprisingly) very low; some major issues 'flagged' at the European level (SWIFT, PNR, DNA) are hardly pursued.

7. Good practices

[180]. As noted, the ICO does good work in terms of issuing guides and leaflets etc. (even if not everyone will always agree with all he says), and raising data protection awareness generally.

[181]. The ICO is also undoubtedly regarded as an important advisor to public and private bodies, and will claim to have had a significant impact on Government- and private-sector policies and practices - although again, he has been criticised for sometimes accepting (or seeming to endorse) dubious practices, e.g. in his advice on the sharing of personal data on children, which suggested that children from the age of 12 could consent to this without a need to involve the parents.[129]

8. Miscellaneous

[182]. The issues in the UK are complex, both in law and in practice. This report can only provide a basic insight into them. It should also be stressed that some (perhaps many) of the critical remarks made in this report could equally be made in respect of other countries, and other DPAs - but the authors of those other reports may have approached their task differently, less critical. Care should therefore be taken in drawing comparative conclusions too easily or quickly from this report.

[129] See: ARCH (Action on Rights for Children), *A Comparative Study Of The Law Relating To 'Informed Consent' To Sharing Children's Personal Data*, study supported by the Nuffield Foundation, due February 2009.

Annexes

Annex 1 – Tables and Statistics[130]

	2000	2001	2002	2003	2004	2005	2006	2007
Budget of data protection authority	£ 4,694,240	£ 5,258,686	£6,703,642	£8,246,622	£10,562,113	£12,982,269	£15,983,027	£9,924,274
Staff of data protection authority	114	126	157	198	208	225	245	262
Number of procedures (investigations, audits etc.) initiated by data protection authority at own initiative								

[130] For all statistical information, see ICO Annual Reports 2000 – 2007, available at: http://www.ico.gov.uk/tools_and_resources/document_library/corporate.aspx (26.01.2009).

Number of data protection registrations[131]	243, 681	220,455	198,519	211,251	251,702	259,296	n.a.	287,000
Number of renewals	38, 354	3,987	46,219	124,782	194,828	225,257	240,000	n.a.
Number of New Applications	25,012	52,642	99,637	110,451	63,942	40,932	36,000	n.a.
Number of data protection approval procedures								
Number of complaints received by data protection authority	5,166	8,875	12,479	12,001	11,664	19,460	22,059	23,988
Number of complaints upheld by data protection authority								

[131] Number of Total Register Entries

Follow up activities of data protection authority, once problems were established (please disaggregate according to type of follow up activity: settlement, warning issued, opinion issued, sanction issued etc.)								
Sanctions and/or compensation payments in data protection cases (please disaggregate between court, data protection authority, other authorities or tribunals etc.) in your country (if possible, please disaggregate between sectors of society and economy)								
Range of sanctions and/or compensation in your country (Please disaggregate according to type of sanction/compensation)								

Any other tables or statistics relevant for assessment of effectiveness of data protection, where available

Annex 2 – Case Law

Please present at least 5 cases on data protection from courts, tribunals, data protection authorities etc. (criteria of choice: publicity, citation in media, citation in commentaries and legal literature, important sanctions) in your country, if available (please state it clearly, if less than 5 cases are available)

Case title	Michael John Durant v Financial Services Authority
Decision date	8 December 2003
Reference details (reference number; type and title of court/body; in original language and English [official translation, if available])	Case No: B2/2002/2636 Court of Appeal (Civil Division) [2003] EWCA Civ 1746; [2003] WL 22826914
Key facts of the case (max. 500 chars)	Mr Durant was a client of Barclays Bank. There was litigation between them, which he lost in 1993. Thereafter he sought disclosure of various records in connection with the dispute in order to re-open his claims. He sought assistance from the Financial Services Authority several times, who finally provided copies of electronic files relating to him (some of which were edited so as not to disclose the names of others) but refused to provide manual files on the ground that the information sought was not 'personal' within the definition in s 1(1) of the *Data Protection Act 1998*. Mr. D appealed against this refusal.
Main reasoning/argumentation (max. 500 chars)	Data is 'personal' when it is biographical in a significant sense, and the putative data subject is its focus rather than some other person with whom he may have been involved. The requested information in this case was not 'personal' in this sense. Parliament intended a 'relevant filing system' to apply to manual records only if they are of sufficient sophistication to provide similar ready accessibility as a computerised filing system. The FSA's filing system did not satisfy this at the time. There is a rebuttable presumption that information relating to another should

	not be disclosed without his consent, and the data controller must decide whether the information is necessarily part of the personal data requested. The data controller has a duty to provide information not documents, so can edit third party information where it is not necessary. The discretion conferred by s 7(9) of the Act is general and untrammelled.
Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	What makes 'data', whether held in computerised or manual files, 'personal' within the meaning of the term 'personal data' in s 1(1) of the 1998 Act? What is meant by a 'relevant filing system' in the definition of 'data' in s 1(1) of the 1998 Act? When should a data controller consider it 'reasonable in all the circumstances', under s 7(4)(b) to comply with a data request even when the personal data includes information about another, who has not consented to its disclosure? By what principles would a court be guided in exercising its discretion under s 7(9) of the Act to order a data controller who has wrongly refused a request for information under s 7(1), to comply with the request?
Results (sanctions) and key consequences or implications of the case (max. 500 chars)	The appeal against the FSA was dismissed. Information filed in a way other than with reference to the data subject is not classed as personal data. A consequence of this decision is that the number of DPA access requests is likely to decrease.
Proposal of key words for data base	Personal data, relevant filing system, temp test, edit

Case title	R (on the application of S) v Chief Constable of South Yorkshire; R (on the application of Marper) v Chief Constable of South Yorkshire
Decision date	22 July 2004
Reference details (reference number; type and title of court/body; in original language and English [official translation, if available])	[2004] UKHL 39
Key facts of the case (max. 500 chars)	The police lawfully took fingerprints and DNA samples from the two applicants after each had been arrested and charged. Neither had previous convictions. One of the claimants was acquitted and proceedings against the other were discontinued. Under s 64(1A) of PACE 1984 the police was authorised to retain fingerprints or DNA samples after they had fulfilled the purposes for which they had been taken, and provided that they were not to be used 'except for purposes related to the prevention or detection of crime, the investigation of an offence or the conduct of a prosecution'. In both cases the police refused to destroy the material, relying on a power conferred by the UK Parliament to retain it for use in the detection of crime. The applicants complained that the retention of their fingerprints and DNA sample breaches Art.8, read with Art.14, of the *European Convention on Human Rights*. In 2004 the Appellate Committee of the House of Lords dismissed their case, saying that any interference with private life was justified by the ability of DNA evidence to identify the guilty and exonerate the innocent.
Main reasoning/argumentation (max. 500 chars)	Dismissing the appeal, the Lords held that 1) in respect of the retention of fingerprints, cellular samples and DNA profiles under s 64(1A) of the PACE 1984, Art 8 of the Convention was not engaged. Moreover, there was no free-standing right under Art 14 to non-discrimination and, as art 8 was not engaged, it followed that art 14 was not triggered. While cultural traditions in the UK as to the state storing information about individuals were material in considering the question of objective justification under Art 8(2), they were not material in considering whether Art 8(1) was engaged, which was a question that should receive a uniform interpretation throughout member states, unaffected by different cultural traditions. Rigorous safeguards were in place to protect against the misuse of retained DNA samples, and their retention did not have an impact on the private lives of individuals; 2) the policy of the respondent to retain, save in exceptional cases, all fingerprints, cellular samples and DNA

	profiles taken from those who had been acquitted of criminal offences or against whom proceedings had not been pursued was lawful. The policy was directed to the prevention or detection of crime, the investigation of offences, the facilitation of prosecutions and the speedy exculpation of the innocent as well as the correction of miscarriages of justice.
Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	When people accused of an offence are acquitted or the charge is not pursued, should the State be allowed to retain their fingerprints, cellular samples and DNA profiles and to use them for the purpose of detecting crime?
Results (sanctions) and key consequences or implications of the case (max. 500 chars)	Following the dismissal of their case by the UK House of Lords, the applicants appealed to the European Court of Human Rights. In a Grand Chamber judgment in December 2008, the Court ruled that over 1.6 million DNA and fingerprint samples of innocent people held on UK police databases must be destroyed. In a unanimous ruling, the 17 judges said that Art.8 applied and that retaining the fingerprints, cellular samples and DNA profiles of persons acquitted of offences, or where proceedings had been dropped, breached a person's right to respect for private life.
Proposal of key words for data base	Retention of fingerprints and DNA samples, interference with private life (Art. 8 ECHR), UK Data Protection Act 1998

Case title	*Common Services Agency v Scottish Information Commissioner*
Decision date	09 July 2008
Reference details (reference number; type and title of court/body; in original language and English [official translation, if available])	[2008] UKHL 47
Key facts of the case (max. 500 chars)	In this case, an application was made for the provision of details of leukaemia incidence in children in specific areas of Scotland. The appellant, the Common Services Agency, had refused on the basis that such information constituted 'personal data' within the meaning of the *Data Protection Act 1998*, s.1(1). The applicant then applied to the Scottish Information Commissioner (SIC), for a decision as to whether his request had been dealt with in

	accordance with the *Freedom of Information (Scotland) Act 2002*. The SIC decided that a living individual could be identified from the data so that by virtue of the 1998 Act Sch.1, it could not be disclosed. He decided however that the data could be disclosed in a 'barnadised' form, i.e. after using an anonymisation technique to minimise the risk of individuals being identified.
Main reasoning/argumentation (max. 500 chars)	The House of Lords held that information concerning the incidence of childhood leukaemia in a particular postal area should not be disclosed unless either it could be anonymised so that it was not 'personal data' or could be released in a form which did not contravene one of the data protection principles under the *Data Protection Act 1998.* It was held that no hard and fast rules could be laid down as to what it might be reasonable to ask a public authority to do to put the information which it held into a form which would enable it to be released consistently with the data protection principles. The approach to be used to determine whether release of information in a barnadised form was in accordance with data protection principles was to try to use the barnadisation system to take the data out of the personal category. "Barnardisation" involved a modification rule which added 0, +1, or –1 to all values where the true value lay in the range from 2 to 4 and adding 0 or +1 to cells where the value was 1. 0s were always kept at 0. It did not guarantee against disclosure but aimed to disguise those cells that had been identified as unsafe.
Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	The issues raised by the appeal required a series of questions to be addressed: (a) whether the information which the Commissioner ordered the Agency to release in barnardised form was 'held' by the Agency at the time of his request, the Agency submitting that the process of barnadisation would require the production or making of information that was different from that which was held by it at the time of the request; (b) whether, if it was, information in that form would constitute 'personal data'; (c) whether, if so, its release would be in accordance with the data protection principles; (d) in particular,whether it would meet at least one of the conditions for the processing of personal data in Sch 2 of the *1998 Data Protection Act*; (e) if so, whether the information would also constitute 'sensitive personal data'; (f) if so, whether its release would also meet at least one of the conditions for processing sensitive personal data in Sch 3 of the 1998 Act.
Results (sanctions) and key consequences or implications of the case (max. 500 chars)	The House of Lords remitted the case to the SIC to determine whether the information in question could be sufficiently anonymised for it not to constitute personal data. In the event that the SIC considered that the barnardised information was not sufficiently anonymous to take it beyond the definition of 'personal data' in terms of the 1998 Act, the SIC would need to consider whether disclosure of such information would comply with the data protection principles and, in particular, the requirements for the processing of sensitive personal data in terms

	of the 1998 Act.
Proposal of key words for data base	Personal data, anonymisation of data; UK Data Protection Act 1998

Case title	*The Chief Constables of West Yorkshire, South Yorkshire and North Wales Police v IC*
Decision date	12 October 2005
Reference details (reference number; type and title of court/body; in original language and English [official translation, if available])	Information Tribunal See: http://www.informationtribunal.gov.uk/Decisions/dpa.htm
Key facts of the case (max. 500 chars)	Three appeals arose from the service of three enforcement notices by the Information Commissioner against three Chief Constables, under s.40 *Data Protection Act 1998*, which required the erasure of conviction data held on the Police National Computer (PNC) relating to three individuals. The Information Commissioner stated in the enforcement notices that in continuing to process the relevant conviction data the three Chief Constables of the forces in question as data controllers contravened the Third and Fifth Data Protection principles, and violated Art.8 of the *European Convention on Human Rights*.
Main reasoning/argumentation (max. 500 chars)	The Tribunal considered that in applying the two data protection principles, the protection of the interests of individuals whose data is sought to be retained needed to be balanced against the legitimate pursuit of public safety and/or the prevention of disorder or crime as well as the general protection of the rights and freedom of others insofar as there is an overlap between those concepts. The Tribunal held that retention of conviction data fell squarely within the concept of 'operational police purposes' as well as the specific purpose descriptions pertaining to the prevention and detection of crime as well as the apprehension and prosecution of offenders which featured in the Register of Particulars applicable in the three cases. However, it held that data which has been kept for longer than necessary for any of the 'operational police purposes' could be regarded as having been kept for an excessive period. It noted however that the factors to be weighed in the balance in applying the Third and Fifth Data Protection Principles may have differing degrees of weight from those which would apply with regard to 'operational police purposes'. It held that, just as

	the purposes differ, so will the factors with regard to a proper consideration of whether the data is relevant and/or its retention is excessive; and/or whether the data is kept longer than is necessary, no matter what the purpose. The Tribunal accepted that Article 8(1) ECHR would be engaged with regard to conviction data. However, it found that the data in this case fell within Article 8(2), since retention was clearly in accordance with the law and related to the interests listed in Article 8(2).
Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	Whereas in the case of *R (Marper) v Chief Constable of the South Yorkshire*, it had been held by UK courts that DNA and finger print information held on the database was not information that engaged Article 8(1), the Tribunal held that conviction data constitutes the clearest form, if not one of the most vivid forms of personal history, and accepted that Article 8(1) would be engaged with regard to conviction data, but that it fell within one of the exceptions under Art. 8(2).
Results (sanctions) and key consequences or implications of the case (max. 500 chars)	The Tribunal took the view that the Commissioner was entitled to issue Enforcement Notices on the material he had on the facts of each of the cases but, given the wider range of material put before it, the Tribunal was able to review the underlying determinations of fact and thereby exercised its right to review the Notices. It substituted new Enforcement Notices requiring the conviction data to be 'stepped down' so that it could only be processed by Chief Constables for their own use subject to the rules in the 'Association of Chief Police Officers' (ACPO) Code of Practice.
Proposal of key words for data base	Retention of conviction data, Police National Computer, UK Data Protection Act 1998

Please attach the text of the original decisions in electronic format (including scanned versions as pdf).

Case title	*The Chief Constable of Humberside and The Chief Constable of Staffordshire Police and The Chief Constable of Northumbria Police and The Chief Constable of West Midlands Police and The Chief Constable of Greater Manchester Police v Information Commissioner*
Decision date	21 July 2008

Reference details (reference number; type and title of court/body; in original language and English [official translation, if available])	Information Tribunal See: http://www.informationtribunal.gov.uk/Decisions/dpa.htm
Key facts of the case (max. 500 chars)	Following the findings of the Tribunal in the case of *The Chief Constables of West Yorkshire, South Yorkshire and North Wales v Information Commissioner* a fourth code of practice was implemented by the Association of Chief Police Officers (ACPO) in order to provide guidance which is in line with the *Data Protection Act 1998* (DPA) relating to retention of personal information on the Police National Computer (PNC). This code of practice was not endorsed by the Information Commissioner (IC) and led to five enforcement notices requiring the erasure of the conviction data of five individuals, after requests by the Criminal Records Bureau (CRB) for standard and enhanced certificates. The IC took enforcement action because he considered that the continuing retention of the information breached the Third and Fifth Data Protection Principles (the DPPs) set out in Schedule 1 to the *Data Protection Act 1998*. In effect the IC considered in each case that the information was irrelevant and excessive in relation to the purposes for which it was held, and that it had been held for longer than necessary.
Main reasoning/argumentation (max. 500 chars)	The Tribunal considered the purposes of the Appellants in the context of the third and fifth data protection principles. Whereas the IC argued that prevention and detection of crime, the investigation and apprehension of offenders, and the maintenance of law and order are the 'core' police purposes and must be taken into account in applying DPP3 and DPP5, the Home Office argued that all the notified purposes must be taken into account. The Tribunal stated that the extent to which the purpose(s) for which the police are registered under the DPA would be pursued if they provided all conviction data to other bodies such as the CRB was not clear. Therefore the Tribunal found that the police should only process data for their core purposes. In data protection terms this processing requires holding criminal intelligence on the PNC for so long as it is necessary for the police's core purposes. Chief Constables cannot be expected to incorporate other bodies' purposes as part of their own even though there may be some common objectives, like the prevention of crime.
Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	The Tribunal accepted the IC's submissions that the third and the fifth principles should be approached by reference to whether the continued retention of the data is necessary (in the sense of being reasonably necessary for police purposes), and whether it is proportionate (that is, whether the purposes pursued justify the interference with the rights of the data subjects).

Results (sanctions) and key consequences or implications of the case (max. 500 chars)	The Tribunal held that there was no error in law in issuing the Enforcement Notices and also stated that the IC's decision to take enforcement action under s.40 DPA was a legitimate and proper exercise of his discretion. Therefore there was no proper basis for the Tribunal to overturn that exercise. It upheld the five enforcement notices and dismissed the appeal.
Proposal of key words for data base	Retention of conviction data, Police National Computer, Enforcement Notice, UK Data Protection Act 1998